

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Kazutoshi KOBAYASHI, et al.

Application. No.: TBD

Filed: December 12, 2003

:
:
:
:
:
:

Group Art Unit: TBD

Examiner: TBD

Title: An Anonymous Electronic Funds Transfer System and Method, and Anonymous Shipping System and Method

CLAIM FOR PRIORITY

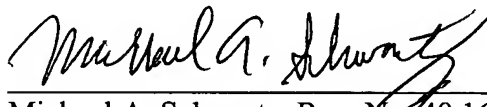
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

A certified copy of corresponding Japanese Application No. 2003-047798, filed February 25, 2003 is attached. It is requested that the right of priority provided by 35 U.S.C. 119 be extended by the U.S. Patent and Trademark Office.

Respectfully submitted,

Date: December 12, 2003



Michael A. Schwartz, Reg. No. 40,161
Swidler Berlin Shereff Friedman, LLP
3000 K Street, NW, Suite 300
Washington, DC 20007-5116

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 2月25日
Date of Application:

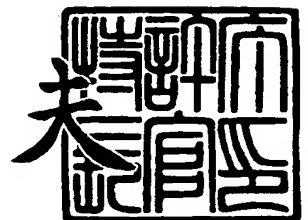
出願番号 特願2003-047798
Application Number:
[ST. 10/C]: [JP2003-047798]

出願人 富士通株式会社
Applicant(s):

2003年10月15日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



【書類名】 特許願

【整理番号】 0252342

【提出日】 平成15年 2月25日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 19/00

【発明の名称】 匿名電子決済システム及び方法、並びに匿名配送システム及び方法

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県横浜市港北区新横浜 3 丁目 9 番 1 8 号 富士通
コミュニケーション・システムズ株式会社内

【氏名】 小林 和敏

【発明者】

【住所又は居所】 神奈川県横浜市港北区新横浜 3 丁目 9 番 1 8 号 富士通
コミュニケーション・システムズ株式会社内

【氏名】 高橋 清人

【発明者】

【住所又は居所】 神奈川県横浜市港北区新横浜 3 丁目 9 番 1 8 号 富士通
コミュニケーション・システムズ株式会社内

【氏名】 大越 英明

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100070150

【住所又は居所】 東京都渋谷区恵比寿4丁目20番3号 恵比寿ガーデン
プレイスタワー32階

【弁理士】

【氏名又は名称】 伊東 忠彦

【電話番号】 03-5424-2511

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0114942

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 匿名電子決済システム及び方法、並びに匿名配送システム及び方法

【特許請求の範囲】

【請求項 1】 クライアント端末で選択された商品の情報を受信する受信手段と、

オンラインショッピングのウェブサイトで提供される商品に対応して該商品の金額を記憶し、前記クライアント端末で選択された商品に対応して該商品の購入を識別する購入識別子を記憶する記憶手段と、

前記記憶手段に記憶されている商品の金額に基づいて、前記クライアント端末で選択された商品の支払い金額を計算する計算手段と、

前記クレジット会社の指定に応答して、前記指定されたクレジット会社のウェブサイトへの接続指示を、前記購入識別子と前記支払い金額とを含めて前記クライアント端末に送信する送信手段とを備え、

前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である匿名電子決済システムにおけるショッピングモールのサーバ。

【請求項 2】 クライアント端末から供給された支払い金額、商品の購入を識別する購入識別子、並びにクレジットカードを特定する情報を受信する受信手段と、

顧客に対応してクレジットカードを特定する情報及び利用残高を記憶し、前記受信手段により受信されたクレジットカードを特定する情報を有する顧客に対応して商品の購入に関する決済を識別する決済識別子を記憶する記憶手段と、

前記記憶手段に記憶されているクレジットカードを特定する情報のうち前記受信手段により受信されたクレジットカードを特定する情報の残高と、前記受信手段により受信された支払い金額とを比較することにより決済を行う決済手段と、

前記購入識別子と前記決済識別子を含む前記決済手段による決済結果を、前記購入識別子を発行したショッピングモールのサーバに送信する送信手段とを備え、

前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である、及び/又は

前記決済識別子は、クレジット会社のウェブサイトに固有な公開鍵で、前記クライアント端末から供給されたクレジットカードを特定する情報に対応する顧客名が暗号化された顧客名である

匿名電子決済システムにおけるクレジット会社のサーバ。

【請求項 3】 前記決済手段は、前記クライアント端末から供給されるパスワードと、前記記憶手段に記憶されているパスワードとを比較し、

前記送信手段は、比較のたびに、前記制御手段による比較結果を前記クライアント端末に送信する、

請求項 2 記載の匿名電子決済システムにおけるクレジット会社のサーバ。

【請求項 4】 クライアント端末で選択された商品の情報を受信する受信手段と、

オンラインショッピングのウェブサイトで提供される商品に対応して該商品の金額及びサイズを記憶し、前記クライアント端末で選択された商品に対応して該商品の購入を識別する購入識別子を記憶する記憶手段と、

前記記憶手段に記憶されている商品の金額及びサイズに基づいて、前記クライアント端末で選択された商品の支払い金額及び必要容積を計算する計算手段と、

前記配送会社の指定に応答して、前記指定された配送会社のウェブサイトへの接続指示を、前記購入識別子、前記支払い金額及び必要容積を含めて前記クライアント端末に送信する送信手段とを備え、

前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である

匿名配送システムにおけるショッピングモールのサーバ。

【請求項 5】 クライアント端末から供給された支払い金額及び必要容積、商品の購入を識別する購入識別子、並びに顧客情報を受信する受信手段と、

前記受信手段により受信された顧客情報に対応して商品の配送を識別する配送識別子を記憶する記憶手段と、

前記購入識別子と前記配送識別子を含む配送の受け付け結果を、前記購入識別子を発行したショッピングモールのサーバに送信する送信手段とを備え、

前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である、及び/又は

前記決済識別子は、クレジット会社のウェブサイトに固有な公開鍵で、前記クライアント端末から供給されたクレジットカードを特定する情報に対応する顧客名が暗号化された顧客名である

匿名配送システムにおける配送会社のサーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、匿名電子決済システム及び方法、並びに匿名配送システム及び方法に関し、特に、オンラインショップ等を通して商品を購入する際に顧客のプライバシーを保護することができる匿名電子決済システム及び方法、並びに匿名配送システム及び方法に関する。

【0002】

【従来の技術】

インターネットの発展に伴い、オンラインショッピングが普及してきている。このオンラインショッピングでは、セキュリティの確保及びプライバシーの保護が重視される。

【0003】

図1は、従来のオンラインショッピングの流れを説明する図である。はじめに、顧客は、クライアント端末のウェブブラウザから、ショッピングモールのウェブサイトにネットワークを介して接続し、購入を希望する商品を選択する（ステップS101）。この選択に応じて、クライアント端末には、購入する商品の代金がショッピングモールのウェブサイトから通知される（ステップS102）。

【0004】

つぎに、ユーザは、購入者名、住所及びクレジットカード番号等をショッピン

グモールのウェブサイトには供給する（ステップS103）。ショッピングモールのウェブサイトでは、クライアント端末から供給されたクレジットカード番号等をクレジット会社のウェブサイトには供給し、クレジット番号を照会する（ステップS104）。

【0005】

クレジット会社のウェブサイトでは、ショッピングモールのウェブサイトから供給されたクレジットカード番号を照会して、該クレジットカードを利用した商品の購入を許可する（ステップS105）。この許可は、ショッピングモールのウェブサイトを通じて、ユーザのクライアント端末に通知される（ステップS106）。その後、ユーザへの商品の送付、代金請求及び支払い等が行われる。

【0006】

上述した従来のシステムにおいて、セキュリティの確保という観点から、たとえば、クレジットカード情報の入力をショッピングモール（電子商店街）のウェブサイトとは独立させることにより、クレジットカード情報を該ウェブサイトに対して隠蔽する方法が開示されている（たとえば、特許文献1）。

【0007】

また、従来のインターネット取引では、ネットワークを介してデータが転送されるときにセキュリティを確保するため、SSL（Secure Socket Layer）暗号化通信が利用されている。SSL暗号化通信技術を利用することで、通信の傍受による第三者への情報の漏洩を防ぐことができる。

【0008】

【特許文献1】

特開2001-117976号公報

【0009】

【発明が解決しようとする課題】

一方、顧客のプライバシーの保護という観点では、図1に示される、ショッピングモールのウェブサイトとクレジット会社のウェブサイトとの間でSSL暗号化通信技術を利用したデータ通信が行われたとしても、データの発信元又は発信先であるウェブサイトから顧客のプライバシーに関する情報が漏洩する可能性が

未だ残されている。

【0010】

たとえば、ショッピングモールのウェブサイトでは主に商品に関する情報を記憶しており、クレジット会社のウェブサイトでは主に顧客に関する情報を記憶している。しかし、商品の購入に関する決済処理の前後での情報のやり取りの過程で、それぞれのウェブサイトは、知る必要の無い情報を有してしまう可能性がある。たとえば、図1の例では、クレジット会社のウェブサイトでは、顧客が購入した商品に関する情報を入手してしまう場合も考えられる。

【0011】

また、ウェブサイトで購入された商品を顧客に配送することが必要な場合、ショッピングモールのウェブサイトには、住所、氏名、電子メールアドレスといった顧客を特定するための情報が供給される場合がある。これらの情報についても顧客のプライバシーが保護される必要がある。

【0012】

上述したクレジットカードの情報のみを隠蔽する方法では、通信回線以外の手段により顧客に商品を配送する工程について考慮されておらず、情報の隠蔽という面で見ると、現在普及している「料金着払い」配送方式に対して優位性を有さない。

【0013】

オンラインショッピングを利用して商品を購入する際に、ショッピングモールのウェブサイト及びクレジット会社又は配送会社のウェブサイトにおいて顧客のプライバシーが保護されることが望まれている。

【0014】

本発明は、ショッピングモールのウェブサイトとクレジット会社のウェブサイトにおいて顧客のプライバシーを保護することができる匿名電子決済システム及び方法を提供することを目的とする。

また、本発明は、ショッピングモールのウェブサイトと配送会社のウェブサイトにおいて顧客のプライバシーを保護することができる匿名配送システム及び方法を提供することを目的とする。

【0015】

【課題を解決するための手段】

上記目的を達成するため、本発明に係る匿名電子決済システムにおけるショッピングモールのサーバは、クライアント端末で選択された商品の情報を受信する受信手段と、オンラインショッピングのウェブサイトで提供される商品に対応して該商品の金額を記憶し、前記クライアント端末で選択された商品に対応して該商品の購入を識別する購入識別子を記憶する記憶手段と、前記記憶手段に記憶されている商品の金額に基づいて、前記クライアント端末で選択された商品の支払い金額を計算する計算手段と、前記クレジット会社の指定に応答して、前記指定されたクレジット会社のウェブサイトへの接続指示を、前記購入識別子と前記支払い金額とを含めて前記クライアント端末に送信する送信手段とを備え、前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である。

【0016】

また、本発明に係る匿名電子決済システムにおけるクレジット会社のサーバは、クライアント端末から供給された支払い金額及び商品の購入を識別する購入識別子、並びにクレジットカードを特定する情報を受信する受信手段と、顧客に対応してクレジットカードを特定する情報及び利用残高を記憶し、前記受信手段により受信されたクレジットカードを特定する情報を有する顧客に対応して商品の購入に関する決済を識別する決済識別子を記憶する記憶手段と、前記記憶手段に記憶されているクレジットカードを特定する情報のうち前記受信手段により受信されたクレジットカードを特定する情報の残高と、前記受信手段により受信された支払い金額とを比較することにより決済を行う決済手段と、前記購入識別子と前記決済識別子を含む前記決済手段による決済結果を、前記購入識別子を発行したショッピングモールのサーバに送信する送信手段とを備え、前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である、及び/又は前記決済識別子は、クレジット会社のウェブサイトに固有な公開鍵で、前記クライアント端末から供給されたクレジットカードを特定する情報に対応する顧客名が暗号化

された顧客名である。

【0017】

このような匿名電子決済システムによれば、オンラインショッピングのウェブサイト、クレジット会社のウェブサイトにおいて、個々の本質的な役割（商品の提供、決済処理）を行うために必要不可欠な情報以外の情報を選択的に隠蔽することができる。

【0018】

【発明の実施の形態】

以下、本発明の実施の形態を添付図面と対応して詳細に説明する。

第1の実施の形態では、商品を購入するときに、オンラインショッピングのウェブサイトとクレジット会社のウェブサイトにおいて顧客情報が漏洩するのを回避するための匿名電子決済システムとして実現される。

【0019】

また、第2の実施の形態では、商品を配送するときに、オンラインショッピングのウェブサブサイトと配送会社Tのウェブサイトにおいて顧客情報が漏洩するのを回避するための匿名配送システムとして実現される。なお、これらの2つのシステムは、互いに独立なシステムとして実現することができる一方で、互いに連動し合う1つのシステムとして実現することができる。

【0020】

図2は、本発明の第1の実施の形態に係る匿名電子決済システムを示すブロック図である。本匿名電子決済システムは、証明書発行局（CA）1、ショッピングモールのウェブサイトWのウェブサーバ3、クレジット会社Cのウェブサイトのウェブサーバ23及びクライアント端末43から構成される。

【0021】

証明書発行局1は、SSL（Secure Socket Layer）対応のウェブサーバ用のデジタル証明書（以下、サーバIDと呼ぶ）を発行する。本実施の形態では、このサーバIDは、インターネットの利用者に対して、ウェブサイトの運営主体となるクレジット会社Cの実在性を証明する。これにより、クレジット会社Cのウェブサーバ23のブラウザと、クライアント端末43のブラウザ又はショッピン

グモールのウェブサーバ3のブラウザとの間の通信を保護するSSL暗号化通信が実現される。

【0022】

このSSL暗号化通信のために、本実施の形態では、たとえば、日本ベリサイン株式会社により提供されるウェブサーバ向けデジタル証明書発行サービスに対して、クレジット会社Cが登録申請を行うことにより上記サーバIDが予め取得され、ウェブサーバ23にインストールされる。

【0023】

また、証明書発行局1には、クレジット会社Cのウェブサーバ23で生成された公開鍵及び秘密鍵が登録される。さらに、クライアント端末43及びショッピングモールのウェブサーバ3には、ルート(CA)証明書が公開され、それぞれのウェブブラウザにプリインストールされる。

【0024】

ショッピングモールのウェブサイトWにおけるウェブサーバ3(以下、ウェブサーバ3と呼ぶ)は、インターネットを通して、オンラインショッピングサービスをクライアント端末43に提供する。該ウェブサーバ3は、制御部5、入力操作部7、表示部9、送信／受信部11、CD-ROMドライバ13、RAM17、ROM19、データベース(DB)21から構成されている。

【0025】

制御部5は、マイクロプロセッサ等であり、ウェブサーバ3全体の動作を制御する。たとえば、SSL暗号化通信を含めた送信／受信部11に対する通信制御、RAM17及びDB21に対するデータ書き込み／読出し制御、表示部9に対する表示制御等を行う。特に、制御部5は、DB21に記憶されているウェブサーバ3に固有な公開鍵／秘密鍵を使用して、クライアント端末43により選択された商品名を暗号化／復号化する。

【0026】

入力操作部7は、マウス又はキーボード等であり、DB21に記憶されているウェブコンテンツ、商品カタログ、クレジット会社情報等の入力又は更新等を行う。表示部9は、液晶ディスプレイ(LCD)等であり、入力操作部7によるデ

ータ入力又は更新の内容等を表示する。また、表示部 9 は、クレジット会社 C のウェブサイトとの間で SSL 暗号化通信を確立するためのデータのやり取りの内容等を表示する。

【0027】

送信／受信部 11 は、モデム等であり、クライアント端末 43 又はウェブサーバ 23 との間でデータ通信を行う。たとえば、オンラインショッピングサービスに関する商品情報のコンテンツ（図 4 参照）をクライアント端末 43 に送信する。また、ウェブサーバ 23 との間で SSL 暗号化通信を確立し、商品の購入に関する決済結果を受信する。

【0028】

RAM 17 は、制御部 5 による処理データを一時的に記憶する。たとえば、クライアント端末 43 により選択された商品の合計金額、制御部 5 により暗号化された商品名等を記憶する。ROM 19 は、本発明によるウェブサーバ 3 の動作を指示するプログラム等を固定的に記憶する。

【0029】

DB 21 は、磁気ディスク等の大容量の記憶装置であり、ウェブコンテンツ、商品カタログ及びクレジット会社情報等を記憶する。商品カタログは、商品名、商品番号、金額及び仕様等が示された電子情報のカタログである。また、クレジット会社の情報は、会社名、所在地、サービス内容といった簡単な会社紹介等から構成される。

【0030】

また、DB 21 には、一方で、ウェブサーバ 3 に固有な公開鍵及び秘密鍵が記憶されており、他方で、ウェブサーバ 23 との間で SSL 暗号化通信を確立するためのアプリケーションプログラム（ルート証明書）がウェブブラウザにプリインストールされている。

【0031】

さらに、DB 21 は、購入テーブル（図示せず）を記憶する。この購入テーブルは、決済の要求に応答して作成され、購入識別番号に対応して、顧客により選択された（暗号化された）商品名及び合計金額等が登録される。この購入識別番

号とは、オンラインショッピングにおいて、クライアント端末 4 3 による商品の選択時に発行される管理用の番号である。

【 0 0 3 2 】

クレジット会社 C のウェブサイトにおけるウェブサーバ 2 3（以下、ウェブサーバ 2 3 と呼ぶ）は、インターネットを通して、クライアント端末 4 3 により選択された商品の購入に関する決済処理を行う。該ウェブサーバ 2 3 は、制御部 2 5、入力操作部 2 7、表示部 2 9、送信／受信部 3 1、C D - R O M ドライバ 3 3、R A M 3 7、R O M 3 9 及びデータベース（D B） 4 1 から構成されている。

【 0 0 3 3 】

制御部 2 5 は、マイクロプロセッサ等であり、ウェブサーバ 2 3 全体の動作を制御する。たとえば、S S L 暗号化通信を含めた送信／受信部 3 1 に対する通信制御、R A M 3 7 及び D B 4 1 に対するデータ書込み／読出し制御、表示部 2 9 に対する表示制御等を行う。特に、制御部 2 5 は、D B 2 1 に記憶されているウェブサーバ 2 3 に固有な公開鍵／秘密鍵を使用して、決済の対象となる商品を購入した購入者の名前を暗号化／復号化する。

【 0 0 3 4 】

入力操作部 2 7 は、マウス又はキーボード等であり、D B 4 1 に記憶されているウェブコンテンツ、顧客情報等の入力又は更新等を行う。表示部 2 9 は、液晶ディスプレイ（L C D）等であり、入力操作部 2 7 によるデータ入力又は更新の内容等を表示する。また、表示部 2 9 は、クライアント端末 4 3 又はウェブサーバ 3 との間で S S L 暗号化通信を実行するためのデータのやり取りの内容等を表示する。

【 0 0 3 5 】

送信／受信部 3 1 は、モデム等であり、クライアント端末 4 3 又はウェブサーバ 3 との間でデータ通信を行う。たとえば、送信／受信部 3 1 は、クライアント端末 4 3 との間で S S L 暗号化通信を確立し、クレジットカード番号及びパスワードの入力画面のコンテンツ（図 7 参照）を送信する。また、ウェブサーバ 3 との間で S S L 暗号化通信を確立し、商品の購入に関する決済結果を送信する。

【0036】

RAM37は、制御部25による処理データを一時的に記憶する。たとえば、クライアント端末43から供給されたクレジットカード番号及びパスワード、並びに制御部25により暗号化された購入者名等を記憶する。ROM19は、本発明によるウェブサーバ23の動作を指示するプログラム等を固定的に記憶する。

【0037】

DB41は、磁気ディスク等の大容量の記憶装置であり、ウェブコンテンツ、顧客情報等を記憶する。この顧客情報には、たとえば、顧客名に対応して、住所、電話番号、電子メールアドレス、勤務先情報、クレジットカード番号、パスワード、及びカード利用の残高等が記憶される。また、DB41には、一方で、本実施の形態による機能を提供するウェブサーバ23に固有な公開鍵及び秘密鍵が記憶されており、他方で、SSL暗号化通信のために証明書発行局1から供給されたサーバIDがプリインストールされている。

【0038】

さらに、DB41は、決済テーブル（図示せず）を記憶する。この決済テーブルには、商品受け取り番号に対応して、暗号化された商品名、暗号化された顧客名、及び購入識別番号等が対応して記憶される。この商品受け取り番号とは、決済を受け付けるとき（図3、ステップS319）、クライアント端末43に対してウェブサーバ23で発行される管理用の番号である。

【0039】

クライアント端末43は、パーソナルコンピュータ、移動体通信端末或いはPDA（Personal Digital Assistant）等であり、ウェブブラウザを通してウェブサーバ3、23のそれぞれにアクセスする。また、クライアント端末43には、ウェブサーバ23との間でSSL暗号化通信を確立するためのアプリケーションプログラム（ルート証明書を含む）がブラウザにプリインストールされている。

【0040】

また、クライアント端末43には、購入を希望する商品、及び希望するクレジット会社等を選択する（図4及び図5参照）ためのキーボード及びマウス等が設けられている。さらに、クライアント端末43には、ウェブサーバ3、23から

供給されるコンテンツ（図 4 及び図 5 参照）を表示するための液晶ディスプレイ等が設けられている。

【0 0 4 1】

図 3 は、本実施の形態に係る匿名電子決済システム全体の動作を説明する図である。ここでは、図 2 に示された構成と対応して一連の動作が説明される。

【0 0 4 2】

はじめに、顧客は、クライアント端末 4 3 のウェブブラウザに対して、オンラインショッピングモールのウェブサイト W の URL（User Location Resource）である <http://w.com> を入力する（ステップ S 3 0 1）。クライアント端末 4 3 は、URL の入力に応答して、商品情報を表示するためのコンテンツの要求をウェブサイト W に送信する（ステップ S 3 0 2）。

【0 0 4 3】

ウェブサーバ 3 において、制御部 5 は、送信／受信部 1 1 で受信されたコンテンツの要求に応答して、DB 2 1 に記憶されている商品カタログの一部を読み出す。次いで、送信／受信部 1 1 は、制御部 5 により読み出された商品カタログをクライアント端末 4 3 に送信する（ステップ S 3 0 3）。クライアント端末 4 3 では、ウェブサーバ 3 から供給された商品情報が表示される（ステップ S 3 0 4）。

【0 0 4 4】

図 4 は、本実施の形態で利用される商品情報を例示する図である。

この商品情報は、DB 2 1 に記憶されている商品カタログの全部又は一部の情報が DB 2 1 から読み出された情報である。本実施の形態では、商品名に対応して料金のみが示されている。

【0 0 4 5】

この画面には、ウェブサイト W で提供される商品 1 ～ 3 及びその料金が表示されている。顧客は、商品名及び料金に対応して設けられた選択欄のボックスをマウスによりクリックすることで、購入を希望する商品を選択する（ステップ S 3 0 5）。

【0 0 4 6】

また、図4に示される画面には、「決済へ」ボタンが示されている。顧客は、購入希望商品を選択した後に、この決済ボタンを押下する（ステップS306）。クライアント端末43は、決済ボタンの押下に応答して、決済の要求をウェブサーバ3に送信する（ステップS307）。この決済要求には、顧客により選択された商品名が含まれる。

【0047】

ウェブサーバ3において、制御部5は、送信／受信部11で受信された決済の要求に応答して、DB21に記憶されている取扱いクレジット会社の情報を読み出す。次いで、送信／受信部11は、制御部5により読み出されたクレジット会社情報をクライアント端末43に転送する（ステップS308）。クライアント端末43には、ウェブサーバ3から供給されたクレジット会社の情報が表示される（ステップS309）。

【0048】

図5は、本実施の形態で利用されるクレジット会社の情報を例示する図である。このクレジット会社情報は、DB21に記憶されているクレジット会社情報の全部又は一部が読み出された情報である。ここでは、取扱いクレジット会社A、B及びCの名前に対応するボタンと同時に、取扱い配送会社S、Tの名前に対応するボタンも同時に表示されている。この配送会社S、Tは、後述する第2の実施の形態による匿名配送システムで選択される。

【0049】

顧客は、希望するクレジット会社のボタンを押下する（ステップS310）。クライアント端末43のウェブブラウザは、クレジット会社のボタンの押下に応答して、選択されたクレジット会社との接続要求をウェブサーバ3に送信する（ステップS311）。

【0050】

ウェブサイトWのウェブサーバ3において、制御部5は、DB21に記憶されている商品カタログを参照して、ステップS307でクライアント端末43から供給された決済要求に含まれる商品名に対応する料金から合計金額を算出する。

【0051】

また、制御部 5 は、本実施の形態による機能を提供するウェブサーバ 3 に固有な公開鍵を DB 2 1 から読み出し、該公開鍵で該決済要求に含まれる商品名を暗号化する（ステップ S 3 1 2）。商品名が暗号化されることにより、クレジット会社は、顧客が何を購入したかを知ることができないため、顧客のプライバシーが保護される。

【 0 0 5 2 】

さらに、制御部 5 は、DB 2 1 に記憶されている購入テーブルに今回の購入イベントの内容を登録する。具体的には、購入識別番号を発行し、該購入識別番号に対応して、ステップ S 3 1 2 で暗号化された商品名を購入テーブルに登録する。

【 0 0 5 3 】

制御部 5 は、クライアント端末 4 3 のウェブブラウザに対して、ショッピングモールのウェブサイト W (<http://w.com>) とは異なるクレジット会社 C のウェブサイト (<http://c.com>) に対応するウィンドウを開く指示を送信する（ステップ S 3 1 3）。この指示に応じて、クライアント端末 4 3 は、ステップ S 3 1 0 で選択されたクレジット会社 C に対応するウェブサーバ 2 3 との間で SSL 暗号化通信を確立する。

【 0 0 5 4 】

図 6 は、本実施の形態において別ウィンドウを開く指示を示す HTML コンテンツを例示する図である。この HTML コンテンツは、ステップ S 3 1 3 で送信される指示である。

【 0 0 5 5 】

特に、その本文<BODY>には、ウィンドウを開く指示 “window.open()” が示されており、該指示には、新たなウィンドウに対応するウェブサイト (<http://c.com>)、及びステップ S 3 1 2 で供給された合計金額 “¥3015”、暗号化された商品名 “axweilax+qweiadxlw”、及び発行された購入識別番号 “xxxx” が含まれている。

【 0 0 5 6 】

SSL 暗号化通信の確立の手順を簡単に説明する。はじめに、クライアント端

末 43では、ウェブブラウザにプリインストールされているSSL暗号化通信を確立するためのアプリケーションプログラムが起動される。次いで、クライアント端末 43は、アクセス要求をウェブサーバ 23に送信する。このアクセス要求には、利用可能な暗号化方式のリスト等が含まれる。つぎに、ウェブサーバ 23は、該アクセス要求に応答して、リプライをクライアント端末 43に送信する。このリプライには、ウェブサーバ 23により決定された利用暗号方式が含まれる。次いで、ウェブサーバ 23は、サーバ証明書をクライアント端末 43に送付する。このサーバ証明書には、ウェブサーバ 23自身から最上位のルートCAに至るまでの全ての証明書（デジタルID）が含まれる。

【0057】

つぎに、鍵の交換が行われる。クライアント端末 43は、ウェブサーバ 23から供給されたデジタルIDを受信し、これ以降の通信でデータを暗号化するために用いられる鍵を生成する元となる乱数データを生成する。このデータは、ウェブサーバ 23のデジタルIDから得られるサーバ公開鍵により暗号化された上でウェブサーバ 23に送信される。以上から、この時点までに両者の合意の取れている方式に基づいて、暗号化／圧縮処理を経たデータの送信が開始される。

【0058】

クライアント端末 43は、クレジットカード番号及びパスワード入力画面のコンテンツをクレジット会社Cのウェブサーバ 23に要求する（ステップS314）。この要求には、たとえば、ステップS313で受信されたHTMLコンテンツの内容（合計金額、暗号化された商品名、購入識別番号）が含まれる。

【0059】

ウェブサーバ 23の制御部 25は、DB 41に記憶されているクレジットカード情報の入力用のコンテンツを読出す。制御部 25は、該読み出されたコンテンツにステップS314で受信されたHTMLコンテンツに含まれている合計金額及び暗号化商品名を組み込んで、SSL暗号化通信方式に従いクライアント端末 43に送信する（ステップS315）。クライアント端末 43には、ウェブブラウザを通して、クレジット会社Cのウェブサイトに対応するウィンドウが新たに表示される（ステップS316）。

【 0 0 6 0 】

図 7 は、本実施の形態におけるクレジットカード番号及びパスワードの入力画面を例示する図である。この画面には、購入金額合計（税込み）、暗号化された商品名、クレジットカード番号及びパスワードの入力ボックス、さらには、商品の購入を希望するボタン及び購入を拒否するボタンが設けられている。

【 0 0 6 1 】

顧客は、入力操作部 2 7 を使用してクレジットカード番号及びパスワードを入力し（ステップ S 3 1 7）、購入希望ボタンを押下する（ステップ S 3 1 8）。クライアント端末 4 3 は、SSL 暗号化通信方式に従い、ステップ 3 1 7 で入力されたクレジットカード番号及びパスワードをウェブサーバ 2 3 に送信する（ステップ 3 1 9）。

【 0 0 6 2 】

ウェブサーバ 2 3 の制御部 2 5 は、クライアント端末 4 3 から供給されたクレジットカード番号及びパスワードに応じて、決済処理を実行する。具体的には、制御部 2 5 は、DB 4 1 に記憶されている顧客情報を参照して、クライアント端末 4 3 から供給されたクレジットカード番号に対応する残高と、ステップ S 1 1 4 で受信された HTML コンテンツ（図 6 参照）に含まれている合計金額とを比較することにより、購入可能であるか否かを決済する。

【 0 0 6 3 】

また、制御部 2 5 は、DB 4 1 を参照して、クライアント端末 4 3 から供給されたクレジットカード番号に対応する顧客名を、DB 4 1 に記憶されているウェブサーバ 2 3 に固有な公開鍵で暗号化する。顧客の名前が暗号化されたことにより、ウェブサイト W は、今回の購入イベントで購入された商品を誰が購入したかを知ることができないため、顧客のプライバシーが保護される。

【 0 0 6 4 】

さらに、制御部 2 5 は、決済の結果が成功（すなわち OK）であった場合に、商品受け取り番号を発行して、DB 4 1 に記憶されている決済テーブルに今回の決済イベントの内容を登録する（ステップ S 3 2 0）。

【 0 0 6 5 】

次いで、ウェブサーバ23の送信／受信部31は、制御部25の指示に応じて、ショッピングモールのウェブサイトWのウェブサーバ3とのSSL暗号化通信を確立する。この確立は、先のクライアント端末43がウェブサーバ3に代わるだけであり、ステップS313の後に説明された手順と同じ手順による。

【0066】

ウェブサーバ23の制御部25は、SSL暗号化通信の開始に応じて、決済結果をSSL暗号化通信方式に従いウェブサーバ3に通知する（ステップS321）。この決済結果には、決済結果自身（たとえば、OK／NO等）に加えて、決済テーブルに先に登録された商品受け取り番号、暗号化された商品名、暗号化された顧客名、及び購入識別番号が含まれる。

【0067】

ウェブサーバ3は、ウェブサーバ23から供給された決済結果をクライアント端末43に転送する（ステップS322）。クライアント端末43は、ウェブサイトWに対応するウィンドウに決済結果を表示する（ステップS323）。その後、制御部25は、SSL暗号化通信を終了させる。

【0068】

その後、たとえば、商品がインターネット等の通信回線を介して顧客に転送可能な電子情報等である場合、ウェブサーバ3の制御部5は、DB21の購入テーブルを参照して、ステップS321で通知された決済結果に含まれる購入識別番号に対応する暗号化された商品名を、DB21に記憶されているウェブサーバ3に固有な秘密鍵により復号化する。

【0069】

この復号化により、該当する商品は、たとえば、業務委託された業者等により梱包され、商品受け取り番号、暗号化された商品名、暗号化された顧客名を示すラベルが貼り付けられ、クレジット会社Cに発送される。そのとき、ウェブサーバ3からウェブサーバ23に代金が請求される（ステップS324）。

【0070】

クレジット会社Cのウェブサイトでは、受け取った商品のラベルに示されている暗号化された顧客名が入力操作部27等を介して入力される。制御部25は、

該入力された暗号化顧客名を、DB 41 に記憶されているウェブサーバ 23 に固有な秘密鍵で復号化することで顧客名を取得する。

【0071】

次いで、制御部 25 は、DB 41 に記憶されている顧客情報を参照して、該当する顧客名に対応して登録されている電子メールアドレスに商品を転送する（ステップ S 325）。その後、クレジット会社 C は、郵送等により顧客に代金を請求する（ステップ S 326）。顧客は、クレジット会社 C の請求に対して、代金を支払う（ステップ S 327）。クレジット会社 C は、顧客の代金の支払いに応じて、ウェブサイト W を運営している法人又は個人に代金を支払う（ステップ 328）。

【0072】

また、商品が上記電子情報以外の物品である場合、たとえば、後述する第 2 の実施の形態による匿名配送システムの動作（図 12 のステップ S 1208）にリンクすることができる。具体的には、配送会社（図 5 参照）が選択され、該選択された配送会社に氏名及び住所（図 14 参照）が送信されることで、配送の受付処理に移行される。この場合、代金は、着払いにて請求されてもよいし、クレジット会社 C から別途郵送により請求されてもよい。

【0073】

図 8 は、本実施の形態によるショッピングモールのウェブサイト W のウェブサーバ 3 を中心とした動作を説明するフローチャートである。ここでは、クライアント端末 43 又はウェブサーバ 23 のウェブブラウザとのリンクについて説明する。

【0074】

はじめに、ウェブサーバ 3 からクライアント端末 43 に商品情報（図 4 参照）が提供され、表示される（ステップ S 801）。次いで、購入を希望する商品の選択に順次応答して（ステップ S 802）、選択された商品名が RAM 17 に記憶される（ステップ S 803）。

【0075】

つぎに、購入の指示が受信されたとき（ステップ S 804）、クレジット会社

情報が読み出されクライアント端末43に送信される。これにより、クライアント端末43には、クレジット会社の情報(図5参照)が表示される(ステップS805)。

【0076】

つぎに、クライアント端末43でクレジット会社を選択されたとき(ステップS806)、たとえば、図5に示されているウィンドウとは別の小さなウィンドウを表示して、選択の可否が最終的に確認される(ステップS807)。

【0077】

最終確認において、クライアント端末43からの確認OKの指示が受信されたとき(ステップS808)、商品カタログが参照され、ステップS803で記憶された商品名と対応して示されている料金を合計して、購入する商品の合計金額が算出される(ステップS809)。また、ステップS803で記憶された商品名は、ウェブサーバ3に固有な公開鍵で暗号化される(ステップS810)。

【0078】

その後、購入識別番号が発行され、該購入識別番号と、ステップS810で暗号化された商品名とが対応されて購入テーブルに登録される。また、クライアント端末43から確認NG、すなわちキャンセルの指示を受信したとき(ステップS815)、ステップS801に戻る。

【0079】

つぎに、ステップS806で選択されたクレジット会社Cのウェブサイトを別のウィンドウで表示させる指示がクライアント端末43に送信される。本実施の形態では、この指示は、ステップS809で計算された合計金額、並びにステップS810で暗号化された商品名、及び購入識別番号を含むHTMLコンテンツ(図6参照)として送信される(ステップS811)。

【0080】

つぎに、ウェブサーバ23との間でSSL暗号化通信が確立された後、決済通知が受信される。この受信された決済結果がOKを示す場合(ステップS812)、決済結果に含まれている購入識別番号が取得される。

【0081】

上述したように、たとえば、商品が電子情報である場合、購入テーブルに記憶されている暗号化された商品名のうち、該取得された購入識別番号に対応する暗号化された商品名が復号化される。この復号化に応じて、該当する商品は、ウェブサイトWに業務委託された業者によりクレジット会社Cに発送される（ステップS813）。また、決済結果がNOであった場合（ステップS814）、ステップS801に戻る。

【0082】

図9は、本実施の形態によるクレジット会社Cのウェブサイトにおけるウェブサーバ23を中心とした動作を説明するフローチャートである。ここでは、クライアント端末43又はウェブサーバ3のウェブブラウザとのリンクについて説明する。

【0083】

はじめに、SSL暗号化通信が確立された後、クライアント端末43から合計金額、暗号化された商品名及び購入識別番号が受信される（ステップS901）。この受信に応じて、図7に示されるクレジットカード及びパスワードの入力画面のコンテンツが作成される。次いで、この入力画面のコンテンツは、クライアント端末43に表示される（ステップS902）。

【0084】

つぎに、購入を拒否するボタン（図7参照）が押下されたとき、すなわち、顧客により決済処理の実行が拒否されたとき（ステップS903）、ウェブサイトWのウェブサーバ3にNGを示すメッセージが送信され、SSL暗号化通信が終了される（ステップS904）。また、商品を購入するボタン（図7参照）が押下されたとき、クレジットカード番号及びパスワードが受信される（ステップS905）。

【0085】

つぎに、決済処理が実行される。具体的には、購入者情報が参照され、受信されたクレジットカード番号が確認されるとともに、該カード番号に対応する残高が確認される（ステップS906）。その後、ウェブサーバ3とSSL暗号化通信が確立される。

【0086】

決済の結果がOKである場合（ステップS907）、決済テーブルに今回の決済イベントの内容が登録され（ステップS908）、商品受け取り番号等が決済結果とともに通知される（ステップS909）。また、決済の結果がNOである場合（ステップS910）、NGを示すメッセージが決済結果として通知される（ステップS911）。

【0087】

本実施の形態に係るシステムを総括すると、ウェブサーバ3は、特に、DB21、制御部5及び送信／受信部11を有している。DB21は、ショッピングモールのウェブサイトWに固有な暗号化鍵、並びに該ウェブサイトWで提供されている商品の名前及び金額を記憶する。送信／受信部11は、クライアント端末43からの商品の購入に関する決済の要求を受信する。

制御部5は、DB21を参照して、該決済要求に含まれている商品名から購入する商品の合計金額を計算するとともに、DB21に記憶されている公開鍵で該決済要求に含まれている商品名を暗号化する。また、制御部5は、送信／受信部11によりクレジット会社Cの指定が受信されたとき、該指定されたクレジット会社による商品購入の決済処理の実行を指示する。送信／受信部11は、制御部5からの指示に応答して、該暗号化された商品名及び該購入商品の合計金額、並びに購入識別番号を含めて、指定されたクレジット会社Cのウェブサイトへの接続指示をクライアント端末43に送信する。

【0088】

ここで、上記実施の形態では、DB21（購入テーブル）には、購入識別子に対応して、暗号化された商品名が購入イベント毎に登録され（図3のステップS312）、この両情報がクライアント端末43に送信される（図3のステップS313）。その後、ウェブサーバ3では、購入テーブルが参照され、ウェブサーバ23からの決済結果に含まれる購入識別番号に対応する暗号化された商品名が復号化される。

【0089】

これに対して、他の形態として、ステップS312での購入テーブルへの登録

後に、購入識別番号のみを送信することも勿論可能である。この購入識別番号は、ウェブサーバ23側で商品に関する情報との対応が判別不可能であることが必須である。したがって、特別なケースとして、この購入識別番号に代えて、暗号化された商品名そのものが送信されてもよい。この場合、ウェブサーバ3は、後の復号化処理を考慮して、ステップS321で受信される決済結果の内容における暗号化された商品名のデータ位置を予め認識していることが好ましい。

【0090】

いずれにしても、受信された決済結果がどの購入イベントに対応するのかをウェブサーバ3側で判別可能であればよい。したがって、購入テーブルには、クライアント端末43により選択された商品に対応して、該商品の購入を識別する識別子（たとえば、記号列）が記憶されていればよい。

【0091】

なお、購入する商品の数は、本発明を限定するものではない。したがって、ウェブサーバ3の制御部5は、クライアント端末43により選択された1つ又は複数の商品に関する支払い金額を計算する。

【0092】

また、本実施の形態に係るシステムを総括すると、ウェブサーバ23は、特に、DB41、送信／受信部31及び制御部25を有している。DB41は、クレジット会社Cのウェブサイト固有な暗号化鍵、並びに顧客に対応してクレジットカード番号及び利用残高を記憶する。送信／受信部31は、オンラインショッピングのウェブサイトWに固有な暗号化鍵で暗号化された商品名、購入商品の合計金額、購入識別番号及びクレジットカード番号をクライアント端末43から受信する。

制御部25は、DB41に記憶されている顧客情報を参照して、送信／受信部31により受信されたクレジットカード番号に対応する利用残高と、受信された購入商品の合計金額との比較に基づいて決済処理を実行する。また、制御部25は、DB41を参照して、送信／受信部31により受信されたクレジットカード番号に対応する顧客名を、DB41に記憶されている公開鍵で暗号化する。送信／受信部31は、暗号化された商品名、暗号化された顧客名、購入識別番号及び

商品受け取り番号を含む決済の結果をオンラインショッピングのウェブサイトWに送信する。

【0093】

上述したウェブサーバ3に対する他の形態に合わせて、送信／受信部31は、暗号化された商品名に代えて、クライアント端末43により選択された商品に対応付けされた商品の購入を識別する識別子を受信してもよい。

【0094】

また、上記実施の形態では、DB41（決済テーブル）には、商品受け取り番号に対応して、暗号化された顧客名（及び購入識別番号）が決済イベント毎に登録され（図3のステップS320）、これら商品受け取り番号と暗号化された顧客名の両情報がウェブサーバ3に送信される（図3のステップS321）。その後、ウェブサーバ23では、決済テーブルを参照して、ウェブサーバ3から発送される商品のラベルに示される商品受け取り番号に対応する暗号化された顧客名が復号化される。

【0095】

これに対して、他の形態として、ステップS320での決済テーブルへの登録後に、商品受け取り番号のみを送信することも勿論可能である。この商品受け取り番号は、ウェブサーバ3側で顧客を特定する情報との対応が判別不可能であることが必須である。したがって、特別なケースとして、この商品受け取り番号に代えて、暗号化された顧客名そのものが送信されてもよい。

【0096】

いずれにしても、受け取った商品がどの決済イベントに対応する商品であるかをウェブサーバ23側で判別可能であればよい。したがって、決済テーブルには、ステップS319で受信されたクレジットカード番号を有する顧客に対応して、商品の購入に関する決済を識別する識別子（たとえば、記号列）が記憶されていけばよい。

【0097】

このように、購入する商品の情報は、商品情報を所有するウェブサイトWのウェブサーバ3の公開鍵で暗号化され、該サイトWの秘密鍵によってのみ暗号を解

くことができるため、クレジット会社Cのウェブサイトに対して隠蔽される。また、商品を購入する顧客の情報は、クレジット会社Cのウェブサーバ23の公開鍵で暗号化され、該サイトの秘密鍵によってのみ暗号を解くことができたため、ウェブサイトWに対して隠蔽される。したがって、互いのサイトで実行すべき処理のために必要な情報のみを取得して、一連の電子決済を実行することができる。

【0098】

つぎに、本実施の形態に対する機能の拡張について図10を参照して説明する。

図10は、本発明の第1の実施の形態による匿名電子決済システムに対して拡張される機能を説明する図である。この図は、たとえば、第1の実施の形態の図3に示されるステップS316とステップS317の間で、クライアント端末43に表示される画面を示している。この画面は、クレジット会社の認証を行うものである。

【0099】

第1の実施の形態では、クライアント端末43とウェブサーバ23との間には、SSL暗号化通信が確立される。このSSL暗号化通信が開始された場合、ウェブサーバ23では、クライアント端末43の顧客を認識することができる。すなわち、ウェブサーバ23は、ステップS317でパスワード及びクレジットカード番号を受信する前に、顧客のパスワードを認識することができる。

【0100】

DB21は、図10に示される画面のコンテンツを予め記憶している。このコンテンツには、3種類のパスワード1, 2, 3の入力ボックスが設けられており、これらの入力ボックスのそれぞれに対応して、クレジット会社Cからのチェック結果が表示されるボックスが設けられている。

【0101】

クライアント端末43に図10に示される画面が表示されたとき、顧客は3種類のパスワードを入力して、チェックボックスをクリックする。ウェブサーバ23の制御部25は、送信／受信部31により受信された3種類のパスワードのそれぞれと、DB41に記憶されている顧客情報において該当する顧客のパスワー

ドとを比較して、“○”又は“×”等の比較結果を生成する。この比較結果は、送信／受信部31によりクライアント端末43に送信され、図10に示されるパスワードのチェック結果を表示するボックスに表示される。

【0102】

この機能により、顧客は、3種類のパスワードの入力に関して、たとえば、「全て正解」、「全て外れ」及び「1つ正解」となるようなパターンで入力する。さらに、ウェブサーバ23の応答であるチェック結果に対して、期待される結果が得られない場合には、クレジット会社Cの信頼度が低いと判断して、以降の手続きを行わないようにすることができる。

【0103】

なお、クライアント端末43に入力されるパスワードの種類は、本発明を限定するものではない。したがって、ウェブサーバ23の制御部25は、クライアント端末から供給される1つ又は複数のパスワードと、DB41に記憶されている該当する顧客のパスワードとを比較して、比較のたびに、比較結果を生成する。

【0104】

つぎに、本発明の第2の実施の形態による匿名配送システムについて説明する。図3の最後で説明したように、本匿名配送システムは、商品が電子情報以外の物品である場合に、1) クレジット会社Cによる決済処理の後にリンクされる料金後払い方式に対応した配送システムとして実現することができ、また、2) クレジット会社Cによる決済処理を介さない料金着払い方式／後払い方式に対応するシステムとして実現することができる。

【0105】

図11は、本発明の第2の実施の形態による匿名配送システムを示すブロック図である。本匿名配送システムは、第1の実施の形態と同一の証明書発行局1、ショッピングモールのウェブサイトWのウェブサーバ45、配送会社Tのウェブサイトのウェブサーバ65及びクライアント端末85から構成される。

【0106】

ショッピングモールのウェブサイトWにおけるウェブサーバ45（以下、ウェブサーバ45と呼ぶ）は、インターネットを通して、オンラインショッピングサ

ービスをクライアント端末 85 に提供する。該ウェブサーバ 45 は、制御部 47、入力操作部 49、表示部 51、送信／受信部 53、CD-ROM ドライバ 55、RAM 59、ROM 61、データベース (DB) 63 から構成されている。

【0107】

制御部 47 は、マイクロプロセッサ等であり、ウェブサーバ 45 全体の動作を制御する。たとえば、SSL 暗号化通信を含めた送信／受信部 53 に対する通信制御、RAM 59 及び DB 63 に対するデータ書き込み／読出し制御、表示部 51 に対する表示制御等を行う。特に、制御部 47 は、DB 63 に記憶されているウェブサーバ 45 に固有な公開鍵／秘密鍵を使用して、クライアント端末 85 により選択された商品名を暗号化／復号化する。

【0108】

入力操作部 49 は、マウス又はキーボード等であり、DB 63 に記憶されているウェブコンテンツ、商品カタログ、配送会社情報等の入力又は更新等を行う。表示部 51 は、液晶ディスプレイ (LCD) 等であり、入力操作部 49 によるデータ入力又は更新の内容等を表示する。また、表示部 51 は、配送会社 T のウェブサイトとの間で SSL 暗号化通信を確立するためのデータのやり取りの内容等を表示する。

【0109】

送信／受信部 53 は、モデム等であり、クライアント端末 85 又はウェブサーバ 65 との間でデータ通信を行う。たとえば、オンラインショッピングサービスに関する商品情報のコンテンツ (図 4 参照) をクライアント端末 85 に送信する。また、ウェブサーバ 65 との間で SSL 暗号化通信を確立し、商品の配送に関する受付け結果を受信する。

【0110】

RAM 59 は、制御部 47 による処理データを一時的に記憶する。たとえば、クライアント端末 85 により選択された商品の合計サイズ、合計金額、制御部 47 により暗号化された商品名等を記憶する。ROM 61 は、本発明によるショッピングモールサイト W のウェブサーバ 45 の動作を指示するプログラム等を固定的に記憶する。

【0111】

DB63は、磁気ディスク等の大容量の記憶装置であり、ウェブコンテンツ、商品カタログ及び配送会社情報を記憶する。商品カタログは、商品名、商品番号、金額及び仕様等が示された電子情報のカタログである。また、配送会社情報は、会社名、所在地、サービス内容といった簡単な会社紹介等から構成される。

【0112】

また、DB63には、一方で、ウェブサーバ45に固有な公開鍵及び秘密鍵が記憶されており、他方で、ウェブサーバ45との間でSSL暗号化通信を確立するためのアプリケーションプログラム（ルート証明書）がウェブブラウザにプリインストールされている。

【0113】

さらに、DB63は、購入テーブル（図示せず）を記憶する。この購入テーブルは、配送の要求に応答して作成され、購入識別番号に対応して、顧客により選択された（暗号化された）商品名及び該商品の合計サイズ等が登録される。この購入識別番号とは、オンラインショッピングサービスにおけるクライアント端末43による商品の選択時に発行される管理用の番号である。

【0114】

配送会社Tのウェブサイトにおけるウェブサーバ65（以下、ウェブサーバ65と呼ぶ）は、インターネットを通して、クライアント端末43により選択された商品を配送するための手続きを行う。なお、配送会社とは、いわゆるバイク便により商品を配達する宅配業者も含まれる。ウェブサーバ65は、制御部67、入力操作部69、表示部71、送信／受信部73、CD-ROMドライバ75、RAM79、ROM39及びデータベース（DB）83から構成されている。

【0115】

制御部67は、マイクロプロセッサ等であり、ウェブサーバ65全体の動作を制御する。たとえば、SSL暗号化通信を含めた送信／受信部73に対する通信制御、RAM79及びDB83に対するデータ書き込み／読出し制御、表示部71に対する表示制御等を行う。特に、制御部67は、DB83に記憶されているウェブサーバ65に固有な公開鍵／秘密鍵を使用して、商品を購入した購入者の氏

名及び住所を暗号化／復号化する。

【0116】

入力操作部 69 は、マウス又はキーボード等であり、DB 83 に記憶されているウェブコンテンツ、顧客情報等の入力又は更新等を行う。表示部 71 は、液晶ディスプレイ（LCD）等であり、入力操作部 69 によるデータ入力又は更新の内容等を表示する。また、表示部 71 は、クライアント端末 85 又はウェブサーバ 45 との間で SSL 暗号化通信を確立するためのデータのやり取りの内容等を表示する。

【0117】

送信／受信部 73 は、モデム等であり、クライアント端末 85 又はウェブサーバ 45 との間でデータ通信を行う。たとえば、送信／受信部 73 は、クライアント端末 85 との間で SSL 暗号化通信を確立し、氏名及び住所の入力画面のコンテンツ（図 14 参照）を送信する。また、ウェブサーバ 45 との間で SSL 暗号化通信を確立し、商品の配送に関する受付け結果を送信する。

【0118】

RAM 79 は、制御部 67 による処理データを一時的に記憶する。たとえば、クライアント端末 85 から供給された氏名及び住所、並びに制御部 67 により暗号化された氏名及び住所等を記憶する。ROM 81 は、本発明による配送会社 T のウェブサーバ 65 の動作を指示するプログラム等を固定的に記憶する。

【0119】

DB 83 は、磁気ディスク等の大容量の記憶装置であり、ウェブコンテンツ等を記憶する。また、DB 83 には、一方で、本実施の形態による機能を提供するウェブサーバ 65 に固有な公開鍵及び秘密鍵が記憶されており、他方で、SSL 暗号化通信のために証明書発行局 1 から供給されたサーバ ID がプリインストールされている。

【0120】

さらに、DB 83 は、配送テーブル（図示せず）を記憶する。この配送テーブルには、商品配送番号に対応して、暗号化された商品名、暗号化された氏名及び住所、並びに購入識別番号等が対応して記憶される。この商品配送番号とは、配

送を受け付けるときに（図12のステップS1219）、クライアント端末85に対してウェブサーバ65で発行される管理用の番号である。

【0121】

クライアント端末85は、パーソナルコンピュータ、移動体通信端末或いはPDA（Personal Digital Assistant）等であり、ウェブブラウザを通してウェブサーバ45、65のそれぞれにアクセスする。このクライアント端末85は、第1の実施の形態におけるクライアント端末43と同じ構成を有する。

【0122】

図12は、本実施の形態に係る匿名配送システム全体の動作を説明する図である。ここでは、図11に示された構成に基づいて一連の動作が説明される。

【0123】

はじめに、顧客は、クライアント端末85のウェブブラウザに対して、オンラインショッピングモールのウェブサイトWのURL（User Location Resource）であるhttp://w.comを入力する（ステップS1201）。クライアント端末85は、URLの入力に応答して、商品情報を表示するためのコンテンツの要求をウェブサイトWに送信する（ステップS1202）。

【0124】

ウェブサイトWのウェブサーバ45において、制御部47は、送信／受信部53で受信されたコンテンツの要求に응答して、DB63に記憶されている商品カタログの一部を読み出す。次いで、送信／受信部53は、制御部47により読み出された商品カタログをクライアント端末85に送信する（ステップS1203）。クライアント端末85では、ウェブサーバ45から供給された商品情報が表示される（ステップS1204）。図4に示されるように、顧客は、商品名及び料金に対応する選択欄のボックスをマウスでクリックすることで、購入を希望する商品を選択する（ステップS1205）。

【0125】

図4に示される画面には、「決済へ」ボタンが示されている。顧客は、購入希望商品を選択した後に、この決済ボタンを押下する（ステップS1206）。クライアント端末85は、決済ボタンの押下に응答して、決済の要求をウェブサー

バ 4 5 に送信する（ステップ S 1 2 0 7）。この決済要求には、顧客により選択された商品名が含まれる。

【 0 1 2 6 】

ウェブサーバ 4 5 において、制御部 4 7 は、送信／受信部 5 3 で受信された決済の要求に応答して、DB 6 3 に記憶されている取扱い配送会社の情報を読み出す。次いで、送信／受信部 5 3 は、制御部 4 7 により読み出された配送会社の情報をクライアント端末 8 5 に転送する（ステップ S 1 2 0 8）。クライアント端末 8 5 には、ウェブサーバ 4 5 から供給された配送会社の情報が表示される（ステップ S 1 2 0 9）。図 5 に示されるように、顧客は、希望する配送会社のボタンを押下する（ステップ S 1 2 1 0）。クライアント端末 8 5 は、配送会社のボタンの押下に応答して、選択された配送会社との接続要求をウェブサーバ 4 5 に送信する（ステップ S 1 2 1 1）。

【 0 1 2 7 】

ウェブサーバ 4 5 において、制御部 4 7 は、DB 6 3 に記憶されている商品カタログを参照して、ステップ S 1 2 0 7 でクライアント端末 8 5 から供給された決済要求に含まれる商品名に対応する料金から合計金額を算出するとともに、該商品名に対応する寸法から合計サイズを算出する。

【 0 1 2 8 】

また、制御部 4 7 は、本実施の形態による機能を提供するウェブサーバ 4 5 に固有な公開鍵を DB 6 3 から読み出し、該公開鍵で該決済要求に含まれる商品名を暗号化する（ステップ S 1 2 1 2）。商品名が暗号化されることにより、クレジット会社は、顧客が何を購入したかを知ることができないため、顧客のプライバシーが保護される。

【 0 1 2 9 】

さらに、制御部 4 7 は、DB 6 3 に記憶されている購入テーブルに今回の購入イベントの内容を登録する。具体的には、購入識別番号を発行し、該購入識別番号に対応して、ステップ S 1 2 1 2 で暗号化された商品名を購入テーブルに登録する。

【 0 1 3 0 】

制御部 47 は、クライアント端末 85 のウェブブラウザに対して、ショッピングモールのウェブサイト W (<http://w.com>) とは異なる配送会社 T のウェブサイト (<http://t.com>) に対応するウィンドウを開く指示を送信する (ステップ S1213)。この指示に応じて、クライアント端末 85 は、ステップ S1210 で選択された配送会社 T に対応するウェブサーバ 65 との間で SSL 暗号化通信を確立する。この確立の手順は、第 1 の実施の形態で説明されたクライアント端末 43 とクレジット会社 C のウェブサーバ 23 との間での手順と同じである。

【0131】

図 13 は、本実施の形態において別ウィンドウを開く指示を示す HTML コンテンツを例示する図である。この HTML コンテンツは、ステップ S1213 で送信される指示である。

【0132】

特に、その本文<BODY>には、ウィンドウを開く指示 “window.open()” が示されており、該指示には、新たなウィンドウに対応するウェブサイト (<http://t.com>)、及びステップ S1212 で供給された合計金額 “¥3015”、合計サイズ “xxx”、暗号化された商品名 “axweilax+qweiadxlw”、及び発行された購入識別番号 “yyyy” が含まれている。

【0133】

クライアント端末 85 は、氏名及び住所の入力画面のコンテンツを配送会社 T のウェブサーバ 65 に要求する (ステップ S1214)。この要求には、たとえば、ステップ S1213 で受信された HTML コンテンツの内容 (合計金額、合計サイズ、暗号化された商品名、購入識別番号) が含まれる。

【0134】

ウェブサーバ 65 の制御部 67 は、DB 83 に記憶されている氏名及び住所の入力用のコンテンツを読出す。制御部 67 は、該読み出されたコンテンツにステップ S1214 で受信された HTML コンテンツに含まれている合計金額及び暗号化された商品名を組み込んで、SSL 暗号化通信方式に従いクライアント端末 85 に送信する (ステップ S1215)。クライアント端末 85 には、ウェブブラウザを通して、配送会社 T のウェブサイトに対応するウィンドウが新たに表示

される（ステップ S 1 2 1 6）。

【0135】

図 1 4 は、本実施の形態における氏名及び住所の入力画面を例示する図である。この画面には、購入金額合計（税込み）、暗号化された商品名、氏名及び住所の入力ボックス、さらには、商品の配送を希望するボタン及び配送を拒否するボタンが設けられている。

【0136】

顧客は、入力操作部 2 7 を使用して氏名及び住所を入力し（ステップ S 1 2 1 7）、配送希望ボタンを押下する（ステップ S 1 2 1 8）。クライアント端末 8 5 は、S S L 暗号化通信方式に従い、ステップ 1 2 1 7 で入力された氏名及び住所をウェブサーバ 6 5 に送信する（ステップ 1 2 1 9）。

【0137】

ウェブサーバ 6 5 の制御部 6 7 は、クライアント端末 8 5 から供給された氏名及び住所を、D B 8 3 に記憶されているウェブサーバ 6 5 に固有な公開鍵で暗号化する。さらに、制御部 6 7 は、今回の配送の受付けイベントの内容を D B 8 3 に記憶されている配送テーブルに登録する（ステップ S 1 2 2 0）。

【0138】

次いで、ウェブサーバ 6 5 の送信／受信部 7 3 は、制御部 6 7 の指示に応じて、ウェブサーバ 4 5 との S S L 暗号化通信を確立する。この確立は、先のクライアント端末 8 5 がウェブサーバ 4 5 に代わるだけであり、ステップ S 1 2 1 3 の後に説明された手順と同じ手順による。

【0139】

ウェブサーバ 6 5 の制御部 6 7 は、S S L 暗号化通信の開始に応じて、配送の受付けの結果を S S L 暗号化通信方式に従いウェブサーバ 4 5 に通知する（ステップ S 1 2 2 1）。この受付け結果には、受付け結果自身（たとえば、O K / N O 等）に加えて、配送テーブルに先に登録された商品配送番号、暗号化された氏名及び住所、並びに購入識別番号が含まれる。

【0140】

ウェブサーバ 4 5 は、ウェブサーバ 6 5 から供給された受付け結果をクライア

ント端末 8 5 に転送する（ステップ S 1 2 2 2）。クライアント端末 8 5 は、ウェブサイト W に対応するウィンドウに受付け結果を表示する（ステップ S 1 2 2 3）。その後、制御部 6 7 は、SSL 暗号化通信を終了させる。

【0 1 4 1】

その後、ウェブサーバ 4 5 の制御部 4 7 は、DB 6 3 の購入テーブルを参照して、ステップ S 1 2 2 1 で通知された受付け結果に含まれる購入識別番号に対応する暗号化された商品名を、DB 6 3 に記憶されているウェブサーバ 4 5 に固有な秘密鍵で復号化する。この復号化により、該当する商品は、梱包されて、商品配送番号、暗号化された商品名、暗号化された氏名及び住所を示すラベルが貼り付けられた後、配送会社 T に発送される（ステップ S 1 2 2 4）。

【0 1 4 2】

配送会社 T のウェブサイトでは、受け取った商品のラベルに示されている暗号化された氏名及び住所は、入力操作部 6 9 を介して入力される。制御部 6 7 は、該入力された暗号化氏名及び住所を、ウェブサーバ 6 5 の DB 8 3 に記憶されているウェブサーバ 6 5 に固有な秘密鍵で復号化することで、氏名及び住所を取得する。

【0 1 4 3】

次いで、配送会社 T は、この取得された氏名及び住所を宛先として商品を配送する（ステップ S 1 2 2 5）。たとえば、料金着払い方式が採用される場合、配送会社 T は、商品引渡し時に顧客に代金を請求する（ステップ S 1 2 2 6）。顧客は、配送会社 T の請求に対して、代金を支払う（ステップ S 1 2 2 7）。配送会社 T は、顧客の代金の支払いに応じて、ショッピングモールのウェブサイト W を運営している個人又は法人に代金を支払う（ステップ S 1 2 2 8）。

【0 1 4 4】

図 1 5 は、本実施の形態によるショッピングモールのウェブサイト W のウェブサーバ 4 5 を中心とした動作を説明するフローチャートである。ここでは、クライアント端末 8 5 又はウェブサーバ 6 5 のウェブブラウザとのリンクについて説明する。

【0 1 4 5】

はじめに、ウェブサーバ45からクライアント端末85に商品情報（図4参照）が提供され、表示される（ステップS1501）。次いで、購入を希望する商品の選択に順次応答して（ステップS1502）、選択された商品名がRAM59に記憶される（ステップS1503）。

【0146】

つぎに、決済の要求が受信されたとき（ステップS1504）、配送会社情報が読み出され、クライアント端末85に送信される。これにより、クライアント端末85には、配送会社の情報（図5参照）が表示される（ステップS1505）。

【0147】

つぎに、クライアント端末85で配送会社が選択されたとき（ステップS1506）、たとえば、図5に示されているウィンドウとは別の小さなウィンドウが表示されて、選択の可否が最終的に確認される（ステップS1507）。

【0148】

最終確認において、クライアント端末85からの確認OKの指示が受信されたとき（ステップS1508）、商品カタログが参照され、ステップS1503で記憶された商品名と対応して示されている料金が合計されて、購入する商品の合計金額が算出される。

【0149】

また、商品カタログが参照され、ステップS1503で記憶された商品名と対応して示されている商品サイズが合計されて、購入する商品の合計サイズが算出される。さらに、ウェブサーバ45に固有な公開鍵で、ステップS1503で記憶された商品名が暗号化される（ステップS1509）。

【0150】

その後、購入識別番号が発行され、該購入識別番号と、ステップS1510で暗号化された商品名とが対応されて購入テーブルに登録される。一方、クライアント端末85から確認NG、すなわちキャンセルの指示を受信したとき（ステップS1513）、ステップS1501に戻る。

【0151】

つぎに、ステップ S1506 で選択された配送会社 T のウェブサイトを用別のウィンドウで表示させる指示がクライアント端末 85 に送信される。本実施の形態では、この指示は、ステップ S1509 で算出された合計金額及び合計サイズ、並びにステップ S1509 で暗号化された商品名、及び購入識別番号を含む HTML コンテンツ（図 13 参照）として送信される（ステップ S1510）。

【0152】

つぎに、配送会社 T のウェブサイトのウェブサーバ 85 との間で SSL 暗号化通信が確立された場合、配送の受付けに関する通知が受信される。この受信された受付けの結果から購入識別番号が取得される（ステップ S1511）。たとえば、該取得された購入識別番号に対応する商品は、配送会社 T に発送される（ステップ S1512）。また、SSL 暗号化通信が確立されなかった場合（ステップ S1514）、ステップ S1501 に戻る。

【0153】

図 16 は、本実施の形態による配送会社 T のウェブサイトにおけるウェブサーバ 65 を中心とした動作を説明するフローチャートである。ここでは、クライアント端末 85 又はウェブサーバ 45 のウェブブラウザとのリンクについて説明する。

【0154】

はじめに、SSL 暗号化通信が確立された後、クライアント端末 85 から合計金額及び合計サイズ、暗号化された商品名及び購入識別番号が受信される（ステップ S1601）。この受信に応じて、図 14 に示される氏名及び住所の入力画面のコンテンツが作成され、クライアント端末 85 に表示される（ステップ S1602）。

【0155】

つぎに、配送を拒否するボタン（図 14 参照）が押下されたとき、すなわち、顧客により配送の受付け処理の実行が拒否されたとき（ステップ S1603）、ウェブサイト W のウェブサーバ 45 に NG を示すメッセージが送信され、SSL 暗号化通信が終了される（ステップ S1604）。また、商品の配送を指示するボタン（図 14 参照）が押下されたとき、氏名及び住所が受信される（ステップ

S1605)。次いで、ウェブサーバ65に固有な公開鍵で、ステップS1605で受信された氏名及び住所が暗号化される（ステップS1606）。さらに、配送テーブルに今回の受付イベントの内容が登録される。

【0156】

その後、ウェブサーバ45とSSL暗号化通信が確立され、商品配送番号等が受け付け結果とともに通知される（ステップS1507）。

【0157】

本実施の形態に係るシステムを総括すると、ウェブサーバ45は、特に、DB63、制御部47及び送信／受信部53を有している。DB63は、ショッピングモールのウェブサイトWに固有な暗号化鍵、並びに該ウェブサイトWで提供されている商品の名前、サイズ及び金額を記憶する。送信／受信部53は、クライアント端末85からの商品の購入に関する決済の要求を受信する。

制御部47は、DB63を参照して、該決済要求に含まれている商品名から購入する商品の合計金額及び合計サイズを計算するとともに、DB63に記憶されている公開鍵で該決済要求に含まれている商品名を暗号化する。また、制御部47は、送信／受信部53により配送会社Tの指定が受信されたとき、該指定された配送会社による商品配送の受付処理の実行を指示する。送信／受信部53は、制御部47からの指示に応答して、該暗号化された商品名及び該購入商品の合計金額及び合計サイズ、並びに購入識別子を含む、指定された配送会社Tのウェブサイトへの接続指示をクライアント端末85に送信する。

【0158】

ここで、上記実施の形態では、DB（購入テーブル）には、購入識別子に対応して、暗号化された商品名が購入イベント毎に登録され（図12のステップS1212）、この両情報がクライアント端末85に送信される（図12のステップS1213）。その後、ウェブサーバ45では、購入テーブルが参照され、ウェブサーバ65からの受け付け結果に含まれる購入識別番号に対応する暗号化された商品名が復号化される。

【0159】

これに対して、他の形態として、ステップS1212での購入テーブルへの登

録後に、購入識別番号のみを送信することも勿論可能である。この購入識別番号は、ウェブサーバ65側で商品に関連する情報との対応が判別不可能であることが必須である。したがって、特別なケースとして、この購入識別番号に代えて、暗号化された商品名そのものが送信されてもよい。この場合、ウェブサーバ45は、後の復号化処理を考慮して、ステップS1221で受信される決済結果の内容における暗号化された商品名のデータ位置を予め認識していることが好ましい。

【0160】

いずれにしても、受信された決済結果がどの購入イベントに対応するのかをウェブサーバ45側で判別可能であればよい。したがって、購入テーブルには、クライアント端末85により選択された商品に対応して、該商品の購入を識別する識別子（たとえば、記号列）が記憶されていればよい。

【0161】

なお、購入される商品の数は、本発明を限定するものではない。したがって、ウェブサーバ45の制御部47は、クライアント端末85により選択された1つ又は複数の商品に関する支払い金額を計算する。これに応じて、制御部47は、1つ又は複数の商品に対応する必要容積を計算する。

【0162】

また、本実施の形態に係るシステムを総括すると、ウェブサーバ65は、特に、DB83、送信／受信部73及び制御部67を有している。DB83は、配送会社Tのウェブサイト固有な暗号化鍵を記憶する。送信／受信部73は、オンラインショッピングのウェブサイトWに固有な暗号化鍵で暗号化された商品名、購入商品の合計金額及び合計サイズ、購入識別番号、並びに購入者の氏名及び住所をクライアント端末43から受信する。

制御部67は、商品配送番号を発行して、送信／受信部73により受信された購入商品の合計金額及び合計サイズ、並びに氏名及び住所を登録することにより受付処理を実行する。また、制御部67は、送信／受信部73により受信された氏名及び住所を、DB83に記憶されている公開鍵で暗号化する。送信／受信部73は、暗号化された商品名、購入識別番号、暗号化された氏名及び住所、並

びに商品配送番号を含む受付けの結果をオンラインショッピングのウェブサイト W に送信する。

【0163】

上述したウェブサーバ 45 に対する他の形態に合わせて、送信／受信部 73 は、暗号化された商品名に代えて、クライアント端末 85 により選択された商品に対応付けされた商品の購入を識別する識別子を受信してもよい。

【0164】

また、上記実施の形態では、DB 83（配送テーブル）には、商品配送番号に対応して、暗号化された氏名及び住所（並びに購入識別番号）が受付イベント毎に登録され（図 12 のステップ S 1220）、これら商品配送番号と暗号化された氏名及び住所の両者が、ウェブサーバ 45 に送信される（図 12 のステップ S 1221）。その後、ウェブサーバ 65 では、配送テーブルが参照され、ウェブサーバ 45 から発送される商品のラベルに示される商品配送番号に対応する暗号化された氏名及び住所が復号化される。

【0165】

これに対して、他の形態として、ステップ S 1220 での配送テーブルへの登録後に、商品配送番号のみを送信することも勿論可能である。この商品配送番号は、ウェブサーバ 45 側で顧客の情報（氏名及び住所等）との対応が判別不可能であることが必須である。したがって、特別なケースとして、この商品配送番号に代えて、暗号化された氏名及び住所そのものが送信されてもよい。

【0166】

いずれにしても、受け取った商品がどの配送の受付けイベントに対応するのかをウェブサーバ 65 側で判別可能であればよい。したがって、配送テーブルには、ステップ S 1219 で受信された顧客の情報に対応して、商品の配送を識別する識別子（たとえば、記号列）が記憶されていればよい。

【0167】

このように、購入する商品の名前は、商品情報を所有するウェブサイト W のウェブサーバ 45 の公開鍵で暗号化され、該サイト W の秘密鍵によってのみ暗号を解くことができるため、配送会社 T のウェブサイトに対して隠蔽される。また、

商品の購入者の氏名及び住所は、配送会社 T のウェブサーバ 6 5 の公開鍵で暗号化され、該サイトの秘密鍵によってのみ暗号を解くことができたため、ウェブサイト W に対して隠蔽される。したがって、互いのサイトで実行すべき処理のために必要な情報のみを取得して、一連の配送の手続きを実行することができる。

【 0 1 6 8 】

なお、上述した第 1 及び第 2 の実施の形態では、SSL 暗号化通信機能を含むシステムとしてそれぞれ実現されている。本発明は、SSL 暗号化通信により限定されるものではない。

【 0 1 6 9 】

なお、本発明の匿名電子決済システム及び匿名配送システムは、この匿名電子決済システム及び匿名配送システムのそれぞれを機能させるためのプログラムによっても実現される。このプログラムは、たとえば、CD-ROM 等のコンピュータで読取り可能な記録媒体に格納されている。

【 0 1 7 0 】

ウェブサーバ 3, 4 5 を機能させるためのプログラムが格納される記録媒体は、図 2 (図 1 1) に示される ROM 1 9, 6 1 そのものであってもよいし、また、外部記憶装置として CD-ROM ドライバ 1 3, 5 5 等のプログラム読み取り装置が設けられ、そこに挿入することで読取り可能な CD-ROM 1 5, 5 7 等であってもよい。

【 0 1 7 1 】

同様に、ウェブサーバ 2 3 (6 5) を機能させるためのプログラムが格納される記録媒体は、図 2 (図 1 1) に示される ROM 3 9 (8 1) そのものであってもよいし、また、外部記憶装置として CD-ROM ドライバ 3 3 (7 5) 等のプログラム読み取り装置が設けられ、そこに挿入することで読取り可能な CD-ROM 3 5 (7 7) 等であってもよい。

また、上記記録媒体は、磁気テープ、カセットテープ、フロッピー（登録商標）ディスク、ハードディスク、MO/MD/DVD 等、又は半導体メモリであってもよい。

【 0 1 7 2 】

本発明は、上述された実施の形態の内容を整理して、付記として開示される。

(付記 1) クライアント端末で選択された商品の情報を受信する受信手段と、
オンラインショッピングのウェブサイトで提供される商品に対応して該商品の
金額を記憶し、前記クライアント端末で選択された商品に対応して該商品の購入
を識別する購入識別子を記憶する記憶手段と、

前記記憶手段に記憶されている商品の金額に基づいて、前記クライアント端末
で選択された商品の支払い金額を計算する計算手段と、

前記クレジット会社の指定に応答して、前記指定されたクレジット会社のウェ
ブサイトへの接続指示を、前記購入識別子と前記支払い金額とを含めて前記クラ
イアント端末に送信する送信手段とを備え、

前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で
、前記クライアント端末で選択された商品の名前が暗号化された商品名である
匿名電子決済システムにおけるショッピングモールのサーバ。

(付記 2) 前記受信手段は、前記購入識別子を含む決済の結果を、前記指定さ
れたクレジット会社のウェブサイトから受信する、

付記 1 記載の匿名電子決済システムにおけるショッピングモールのサーバ。

(付記 3) クライアント端末から供給された支払い金額、商品の購入を識別す
る購入識別子、並びにクレジットカードを特定する情報を受信する受信手段と、

顧客に対応してクレジットカードを特定する情報及び利用残高を記憶し、前記
受信手段により受信されたクレジットカードを特定する情報を有する顧客に対応
して商品の購入に関する決済を識別する決済識別子を記憶する記憶手段と、

前記記憶手段に記憶されているクレジットカードを特定する情報のうち前記受
信手段により受信されたクレジットカードを特定する情報の残高と、前記受信手
段により受信された支払い金額とを比較することにより決済を行う決済手段と、

前記購入識別子と前記決済識別子を含む前記決済手段による決済結果を、前記
購入識別子を発行したショッピングモールのサーバに送信する送信手段とを備え

、

前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で
、前記クライアント端末で選択された商品の名前が暗号化された商品名である、

及び/又は

前記決済識別子は、クレジット会社のウェブサイト固有な公開鍵で、前記クライアント端末から供給されたクレジットカードを特定する情報に対応する顧客名が暗号化された顧客名である

匿名電子決済システムにおけるクレジット会社のサーバ。

(付記4) 前記決済手段は、前記クライアント端末から供給されるパスワードと、前記記憶手段に記憶されているパスワードとを比較し、

前記送信手段は、比較のたびに、前記制御手段による比較結果を前記クライアント端末に送信する、

付記3記載の匿名電子決済システムにおけるクレジット会社のサーバ。

(付記5) クライアント端末で選択された商品の情報を受信する受信手段と、オンラインショッピングのウェブサイトで提供される商品に対応して該商品の金額及びサイズを記憶し、前記クライアント端末で選択された商品に対応して該商品の購入を識別する購入識別子を記憶する記憶手段と、

前記記憶手段に記憶されている商品の金額及びサイズに基づいて、前記クライアント端末で選択された商品の支払い金額及び必要容積を計算する計算手段と、

前記配送会社の指定に応答して、前記指定された配送会社のウェブサイトへの接続指示を、前記購入識別子、前記支払い金額及び必要容積を含めて前記クライアント端末に送信する送信手段とを備え、

前記購入識別子は、オンラインショッピングのウェブサイト固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である

匿名配送システムにおけるショッピングモールのサーバ。

(付記6) 前記受信手段は、前記購入識別子を含む配送の受付け結果を、前記指定された配送会社のウェブサイトから受信する、

付記5記載の匿名配送システムにおけるショッピングモールのサーバ。

(付記7) クライアント端末から供給された支払い金額及び必要容積、商品の購入を識別する購入識別子、並びに顧客情報を受信する受信手段と、

前記受信手段により受信された顧客情報に対応して商品の配送を識別する配送識別子を記憶する記憶手段と、

前記購入識別子と前記配送識別子を含む配送の受け付け結果を、前記購入識別子を発行したショッピングモールのサーバに送信する送信手段とを備え、

前記購入識別子は、オンラインショッピングのウェブサイトに固有な公開鍵で、前記クライアント端末で選択された商品の名前が暗号化された商品名である、及び/又は

前記決済識別子は、クレジット会社のウェブサイトに固有な公開鍵で、前記クライアント端末から供給されたクレジットカードを特定する情報に対応する顧客名が暗号化された顧客名である

匿名配送システムにおける配送会社のサーバ。

(付記 8) クライアント端末で選択された商品の情報を受信し、

オンラインショッピングのウェブサイトで提供される商品に対応して該商品の金額を記憶するとともに、前記クライアント端末で選択された商品に対応して該商品の購入を識別する購入識別子を記憶し、

前記記憶されている商品の金額に基づいて、前記クライアント端末で選択された商品の支払い金額を計算し、

前記クレジット会社の指定に応答して、前記指定されたクレジット会社のウェブサイトへの接続指示を、前記購入識別子と前記支払い金額とを含めて前記クライアント端末に送信する匿名電子決済方法。

(付記 9) クライアント端末から供給された支払い金額及び商品の購入を識別する購入識別子、並びにクレジットカードを特定する情報を受信し、

顧客に対応してクレジットカードを特定する情報及び利用残高を記憶するとともに、前記受信されたクレジットカードを特定する情報を有する顧客に対応して商品の購入に関する決済を識別する決済識別子を記憶し、

前記記憶されているクレジットカードを特定する情報のうち前記受信手段により受信されたクレジットカードを特定する情報の残高と、前記受信された支払い金額とを比較することにより決済を行い、

前記購入識別子と前記決済識別子を含む前記決済の結果を、前記購入識別子を発行したショッピングモールのサーバに送信する匿名電子決済方法。

(付記 10) クライアント端末で選択された商品の情報を受信し、

オンラインショッピングのウェブサイトで提供される商品に対応して該商品の金額及びサイズを記憶するとともに、前記クライアント端末で選択された商品に対応して該商品の購入を識別する購入識別子を記憶し、

前記記憶されている商品の金額及びサイズに基づいて、前記クライアント端末で選択された商品の支払い金額及び必要容積を計算し、

前記配送会社の指定に応答して、前記指定された配送会社のウェブサイトへの接続指示を、前記購入識別子、前記支払い金額及び必要容積を含めて前記クライアント端末に送信する匿名電子配送方法。

(付記 1 1) クライアント端末から供給された支払い金額及び必要容積、商品の購入を識別する購入識別子、並びに顧客情報を受信し、

前記受信された顧客情報に対応して商品の配送を識別する配送識別子を記憶し、

前記購入識別子と前記配送識別子を含む配送の受け付け結果を、前記購入識別子を発行したショッピングモールのサーバに送信する匿名配送方法。

【 0 1 7 3 】

【発明の効果】

本発明によれば、オンラインショッピングを利用して商品を購入する際に、ショッピングモールのウェブサイト及びクレジット会社又は配送会社のウェブサイトにおける顧客情報の漏洩を回避することができ、プライバシーが保護される。

【図面の簡単な説明】

【図 1】

従来のオンラインショッピングの流れを説明する図である。

【図 2】

本発明の第 1 の実施の形態に係る匿名電子決済システムを示すブロック図である。

【図 3】

本発明の第 1 の実施の形態に係る匿名電子決済システム全体の動作を説明する図である。

【図 4】

本発明の実施の形態で利用される商品情報を例示する図である。

【図 5】

本発明の実施の形態で利用されるクレジット会社の情報を例示する図である。

【図 6】

本発明の第 1 の実施の形態において別ウィンドウを開く指示を示す HTML コンテンツを例示する図である。

【図 7】

本発明の第 1 の実施の形態におけるクレジットカード番号及びパスワードの入力画面を例示する図である。

【図 8】

本発明の第 1 の実施の形態によるショッピングモールのウェブサイト W のウェブサーバ 3 を中心とした動作を説明するフローチャートである。

【図 9】

本発明の第 1 の実施の形態によるクレジット会社 C のウェブサイトにおけるウェブサーバ 2 3 を中心とした動作を説明するフローチャートである。

【図 10】

本発明の第 1 の実施の形態による匿名電子決済システムに対して拡張される機能を説明する図である。

【図 11】

本発明の第 2 の実施の形態による匿名配送システムを示すブロック図である。

【図 12】

本発明の第 2 の実施の形態に係る匿名配送システム全体の動作を説明する図である。

【図 13】

本発明の第 2 の実施の形態において別ウィンドウを開く指示を示す HTML コンテンツを例示する図である。

【図 14】

本発明の第 2 の実施の形態における氏名及び住所の入力画面を例示する図である。

【図 15】

本発明の第2の実施の形態によるショッピングモールのウェブサイトWのウェブサーバ45を中心とした動作を説明するフローチャートである。

【図 16】

本発明の第2の実施の形態による配送会社Tのウェブサイトにおけるウェブサーバ65を中心とした動作を説明するフローチャートである。

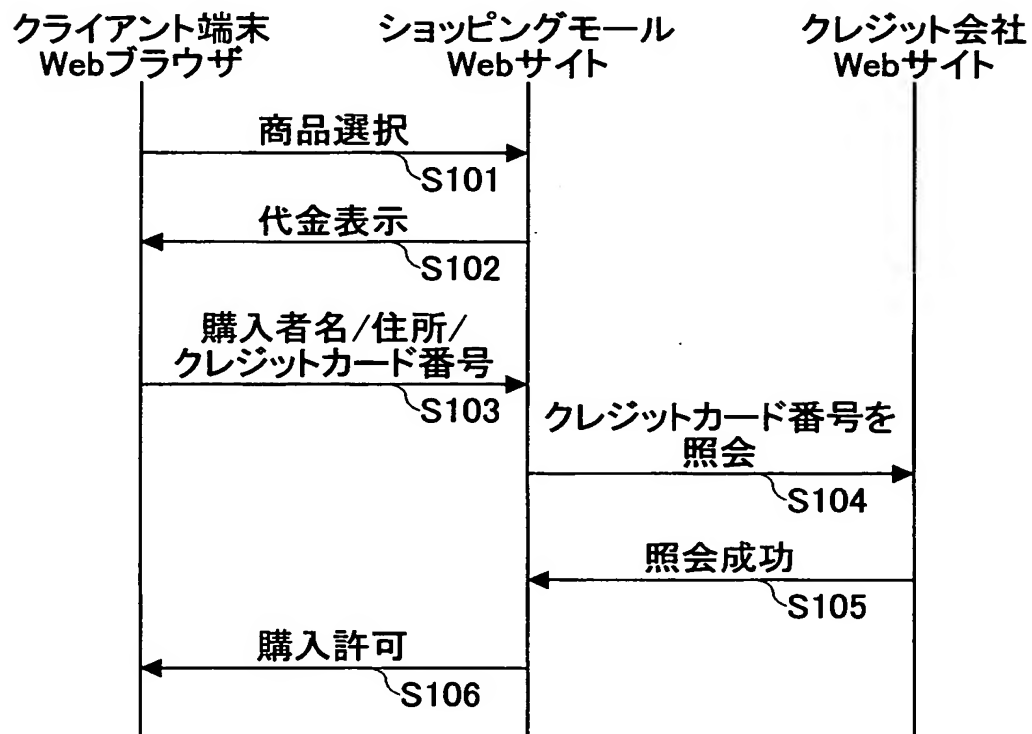
【符号の説明】

- 1：証明書発行局（CA）
- 3，45：ショッピングモールのウェブサーバ
- 5，25，47：制御部
- 7，27，49：入力操作部
- 9，29，51：表示部
- 11，31，53：送信／受信部
- 13，33，55：CD-ROMドライバ
- 15，35，57：CD-ROM
- 17，37，59：RAM
- 19，39，61：ROM
- 21，41，63：データベース
- 23：クレジット会社Cのウェブサーバ
- 65：配送会社Tのウェブサーバ
- 43，85：クライアント端末

【書類名】 図面

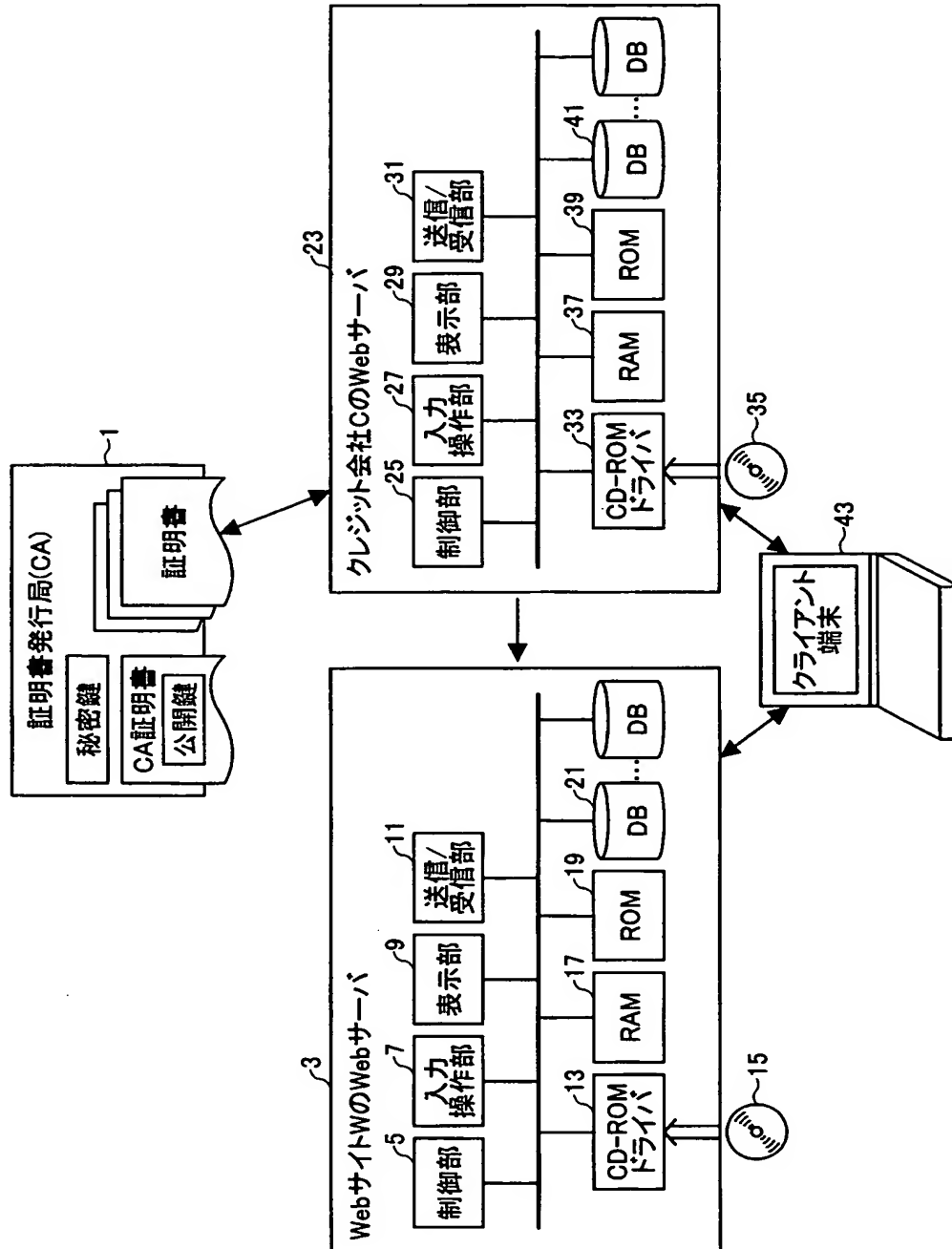
【図 1】

従来のオンラインショッピングの流れを説明する図



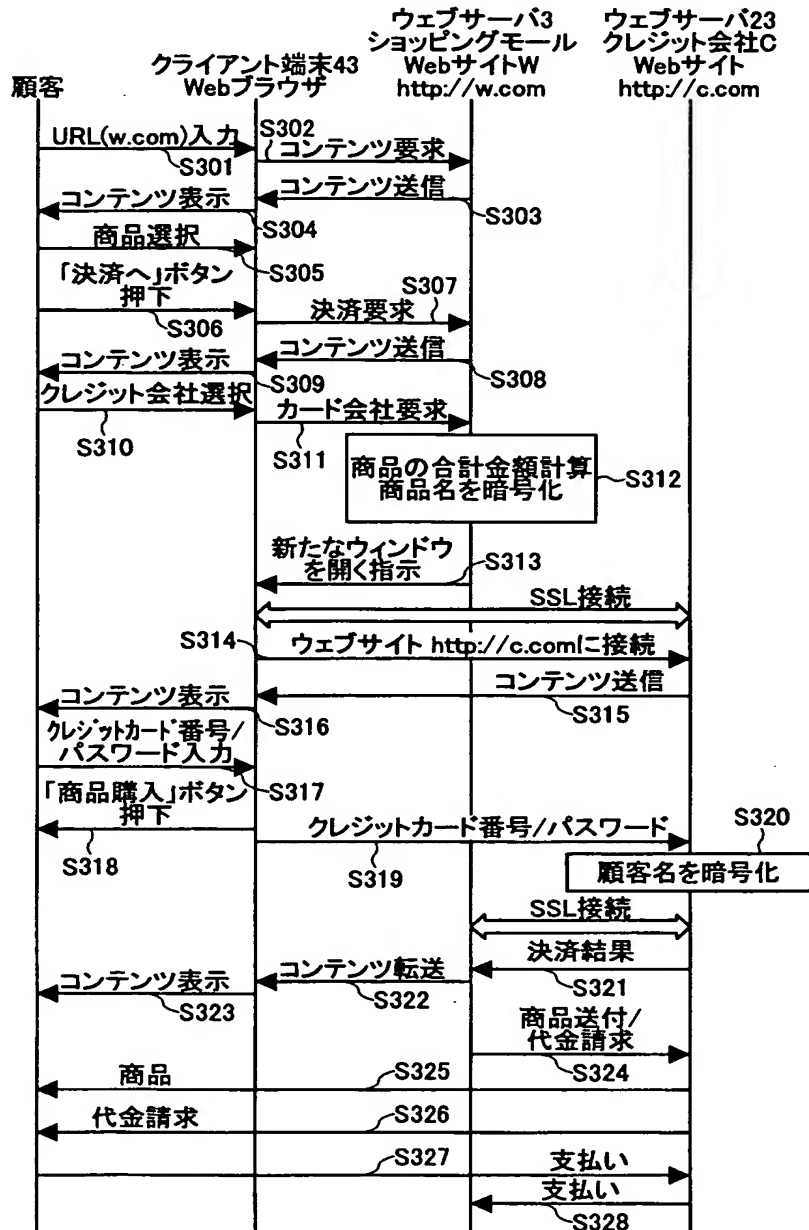
【図 2】

本発明の第1の実施の形態に係る
匿名電子決済システムを示すブロック図



【図3】

本発明の第1の実施の形態に係る
匿名電子決済システム全体の動作を説明する図



【図 4】

本発明の実施の形態で利用される商品情報を例示する図

The image shows a web browser window with a menu bar containing 'ファイル(F)', '編集(E)', '表示(V)', and 'お気に入り(A)'. The main content area displays the title 'WebサイトW' and the instruction '購入希望商品を選択' (Select the product you wish to purchase). Below this, it says '購入する商品を選択してください。' (Please select the product you wish to purchase). A table lists three products with checkboxes for selection. At the bottom, there is a button labeled '決済へ' (Go to payment).

選択	商品名	料金
<input type="checkbox"/>	商品1	¥1,000
<input type="checkbox"/>	商品2	¥2,000
<input type="checkbox"/>	商品3	¥3,000

決済へ

【図 5】

本発明の実施の形態で利用されるクレジット会社の
情報を例示する図

The image shows a web browser window with a menu bar at the top containing 'ファイル(F)', '編集(E)', '表示(V)', 'お気に入り(A)', 'ツール(T)', and 'ヘルプ(H)'. The main content area is titled 'WebサイトW' and contains the text '決済: クレジット会社/配送会社を選択' and 'ご希望のクレジット会社/配送会社を選択してください。'. Below this text are five rectangular buttons arranged vertically: 'クレジット会社A', 'クレジット会社B', 'クレジット会社C', '配送会社S', and '配送会社T'. The browser window has standard window controls (minimize, maximize, close) in the top right corner and a vertical scrollbar on the right side.

【図 6】

本発明の第1の実施の形態において別ウィンドウを
開く指示を示すHTMLコンテンツを例示する図

```
<HTML>
<HEAD>
<TITLE></TITLE>
</HEAD>
<BODY onload=window.open
      ("https://c.com?合計金額=3015
      &暗号化商品名=axweilax+qweiadxlw
      &購入識別番号=xxxx")>

</BODY>
</HTML>
```

【図 7】

本発明の第1の実施の形態におけるクレジットカード
番号及びパスワードの入力画面を例示する図

クレジット会社C

クレジットカード番号+パスワード入力

購入金額合計(税込み) ¥ 3,015

暗号化商品名: axweilax+qweiadxlw

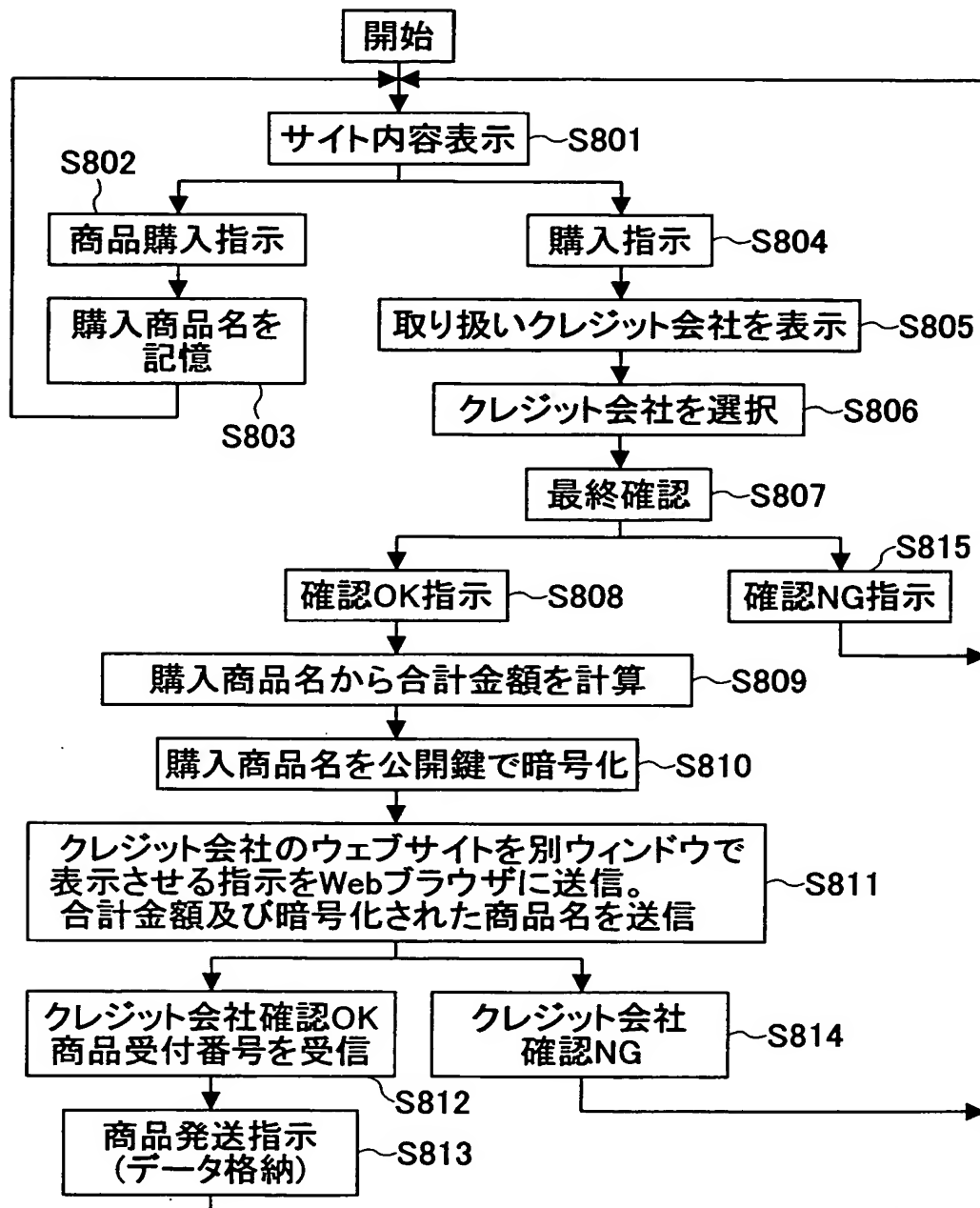
クレジットカード番号	XXXX XXXX XXXX XXXX
パスワード	*****

商品購入

購入拒否

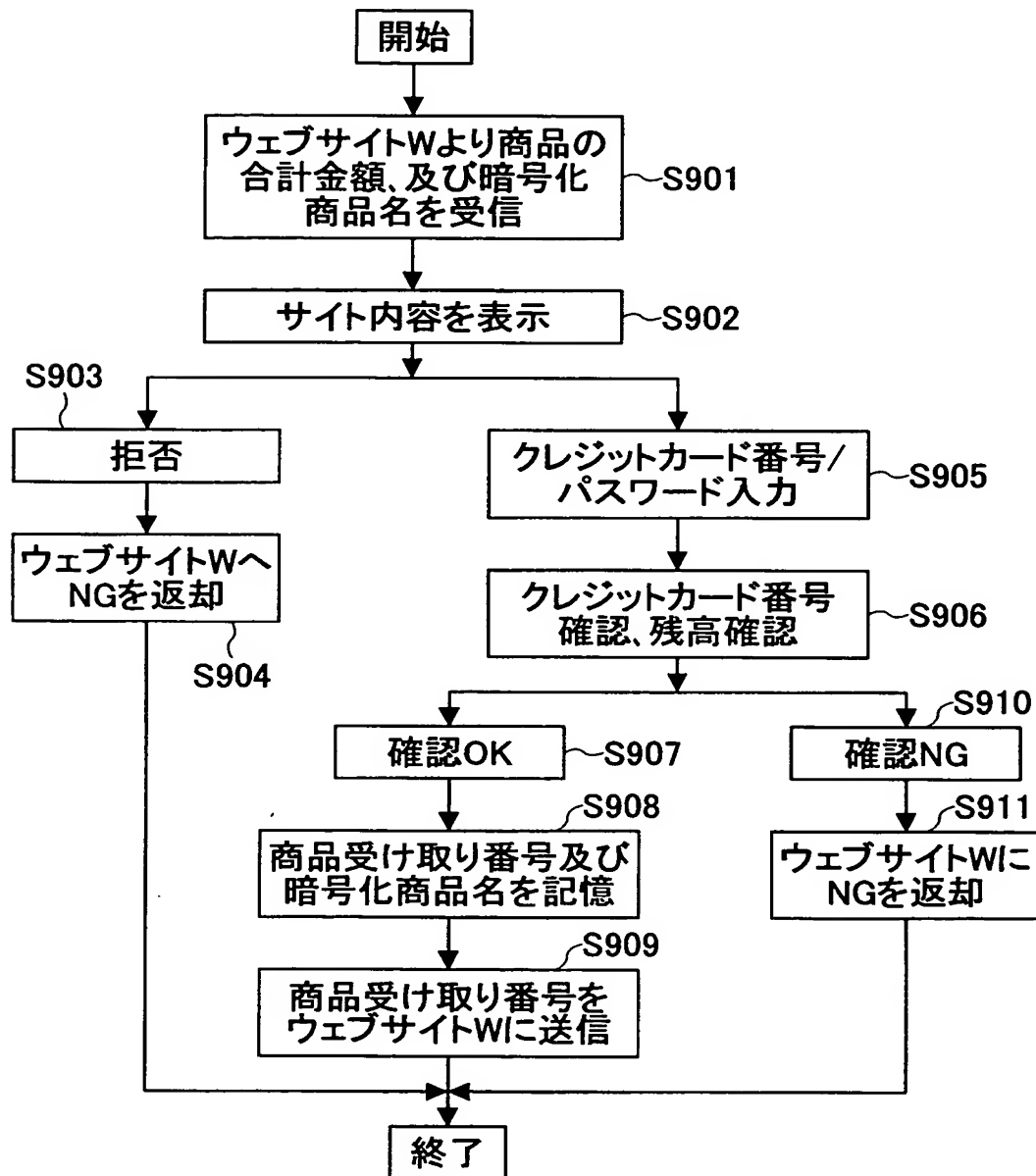
【図 8】

本発明の第1の実施の形態によるショッピングモールのウェブサイトWのウェブサーバ3を中心とした動作を説明するフローチャート



【図 9】

本発明の第1の実施の形態によるクレジット会社Cの
ウェブサイトにおけるウェブサーバ23を中心とした
動作を説明するフローチャート



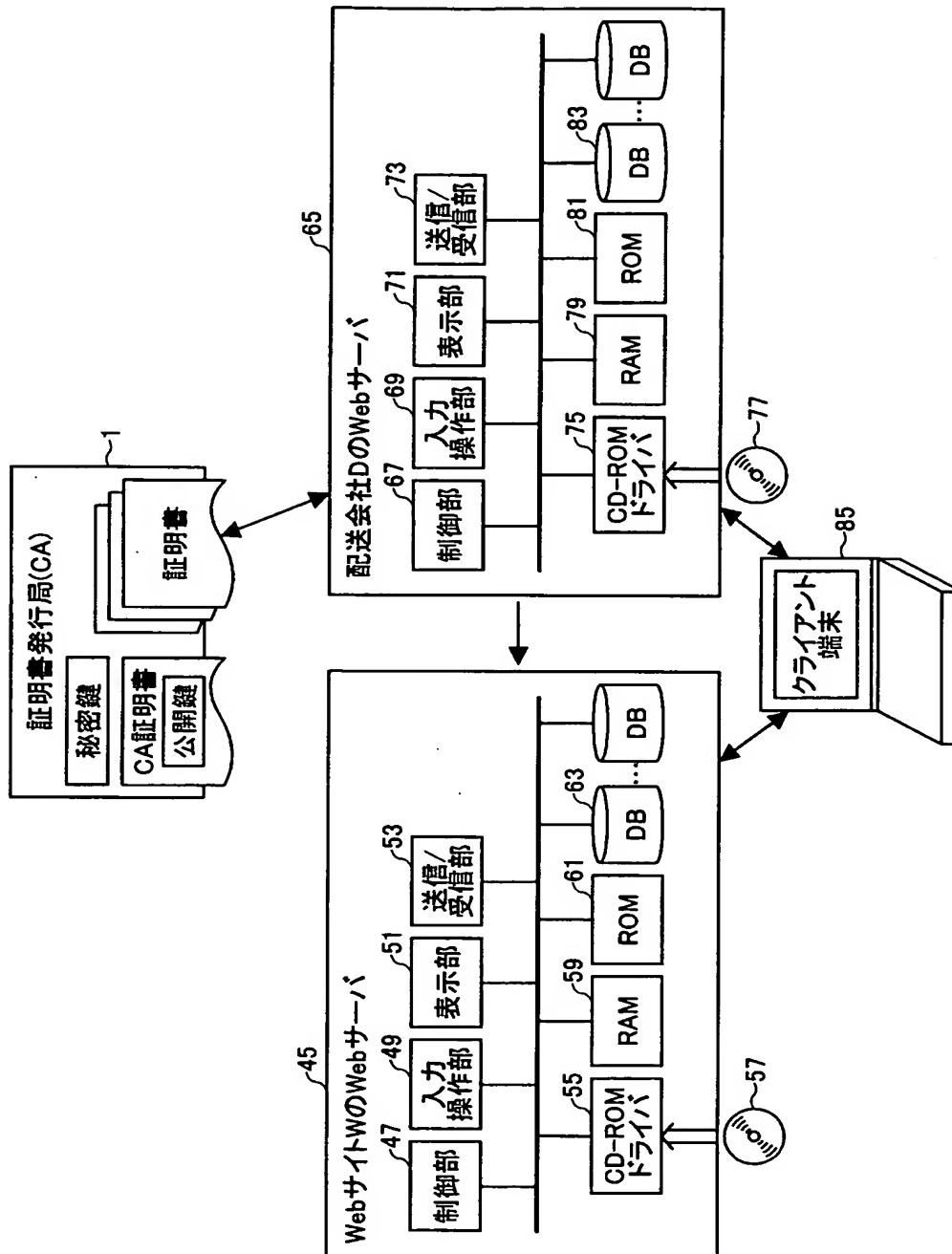
【図 10】

本発明の第1の実施の形態による匿名電子決済システム
に対して拡張される機能を説明する図

クレジットカード番号		
パスワード1	→	×
パスワード2	→	○
パスワード3	→	×
チェック		

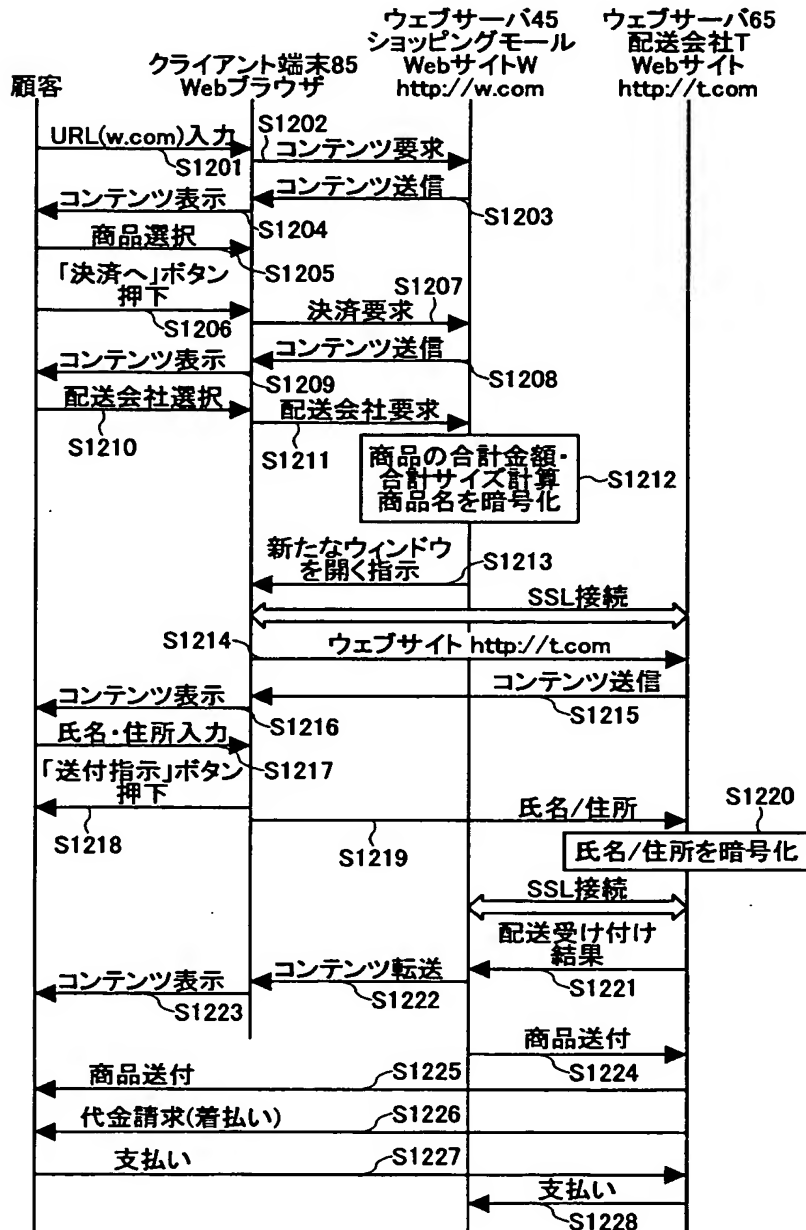
【図 11】

本発明の第2の実施の形態による
匿名配送システムを示すブロック図



【図 12】

本発明の第2の実施の形態に係る
匿名配送システム全体の動作を説明する図



【図 13】

本発明の第2の実施の形態において別ウィンドウを開く指示を示すHTMLコンテンツを例示する図

```
<HTML>
<HEAD>
<TITLE></TITLE>
</HEAD>
<BODY onload=window.open
      ("https://c.com?合計金額=3015
      &合計サイズ=xxx
      &暗号化商品名=axz+yuxle
      &購入識別番号=yyyy")>
</BODY>
</HTML>
```

【図 14】

本発明の第2の実施の形態における
氏名及び住所の入力画面を例示する図

配送会社T

氏名・住所入力

商品名 ax+yuxle

購入金額合計(税込み) ¥ 3,015

送料 ¥400

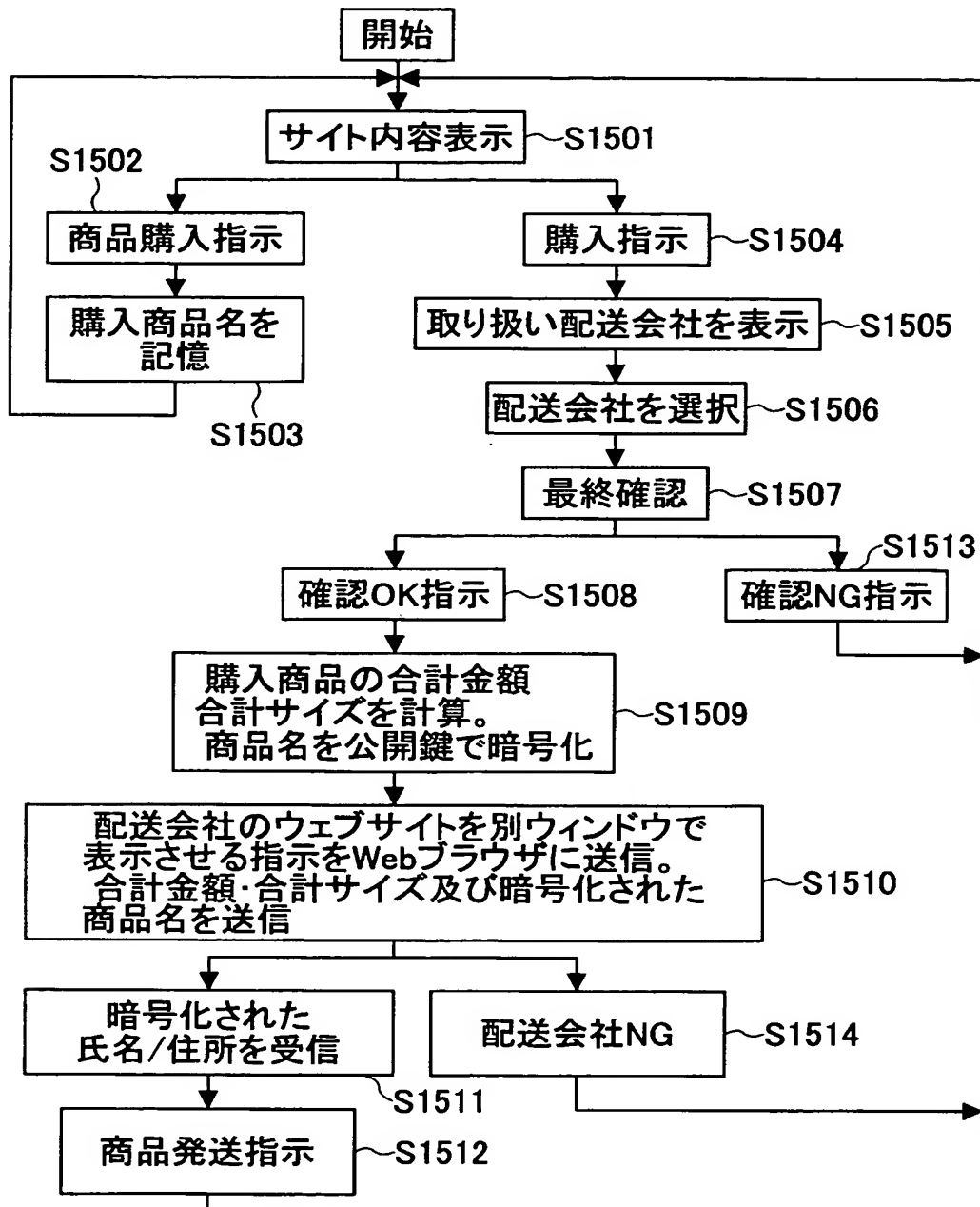
氏名	〇〇 〇〇
住所	神奈川県...

送付指示

送付拒否

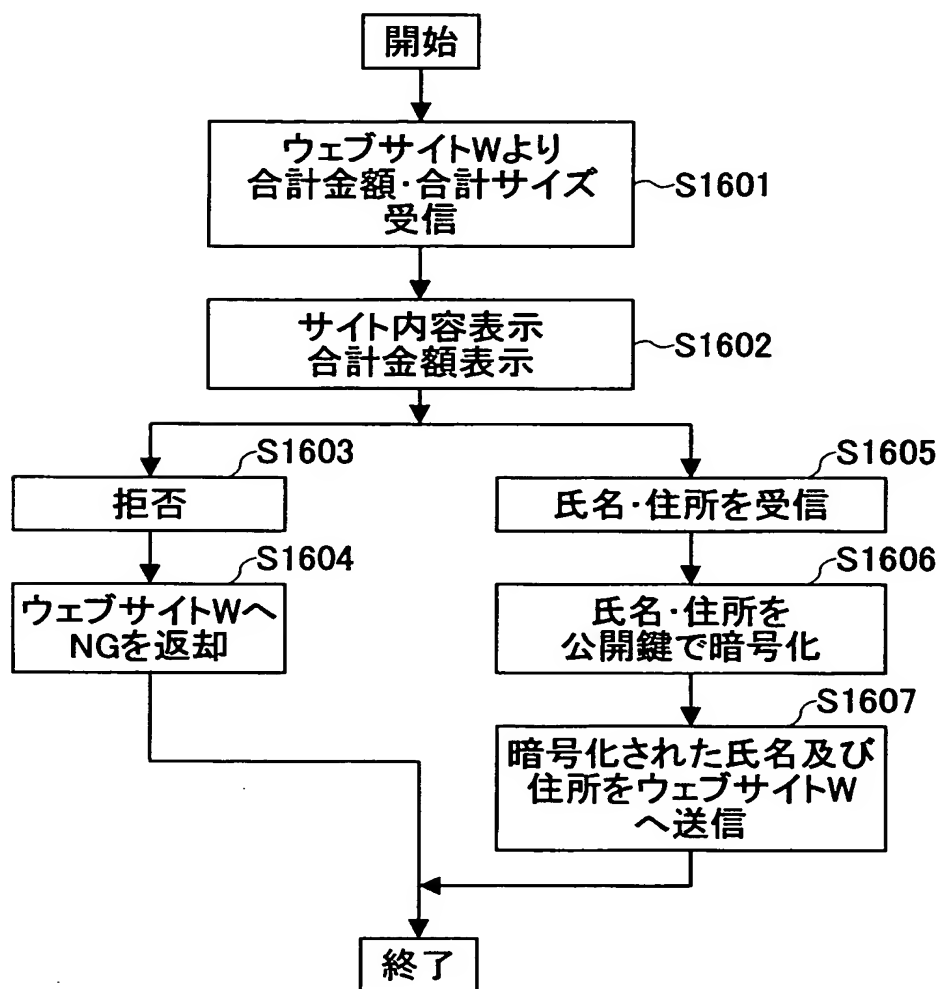
【図15】

本発明の第2の実施の形態によるショッピングモールの
ウェブサイトWのウェブサーバ45を中心とした
動作を説明するフローチャート



【図 16】

本発明の第2の実施の形態による配送会社Tの
ウェブサイトにおけるウェブサーバ65を中心とした
動作を説明するフローチャート



【書類名】 要約書

【要約】

【課題】 オンラインショッピングを利用して商品を購入する際に、ショッピングモールのウェブサイト及びクレジット会社又は配送会社のウェブサイトにおける顧客情報の漏洩を回避する。

【解決手段】 送信／受信部 11 は、クライアント端末 43 で選択された商品の情報を受信する。DB 21 は、オンラインショッピングのウェブサイトで提供される商品の名前に対応して該商品の金額が登録される商品カタログ、及びクライアント端末 43 で選択された商品名に対応して商品の購入を識別する購入識別番号が登録される購入テーブルを記憶する。制御部 5 は、DB 21 の商品カタログを参照して、クライアント端末 43 で選択された商品の合計金額を計算する。送信／受信部 11 は、クレジット会社の指定に応答して、指定されたクレジット会社 C のウェブサイトへの接続指示を、購入識別番号と合計金額とを含めてクライアント端末 43 に送信する。

【選択図】 図 2

特願 2003-047798

出願人履歴情報

識別番号

[000005223]

1. 変更年月日

1996年 3月26日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中4丁目1番1号

氏 名

富士通株式会社